



**UNIVERSITY
OF ICELAND**

The state of cybersecurity vulnerability reporting in Iceland

Þorsteinn Kristinn Ingólfsson

September 2023

M.Sc. thesis
in Software Engineering

The state of cybersecurity vulnerability reporting in Iceland

Þorsteinn Kristinn Ingólfsson

60 ECTS thesis submitted in partial fulfillment of a
Magister Scientiarum degree in Software Engineering

Supervisor
Helmut Neukirchen

M.Sc. Committee
Gerardo Reynaga
Helmut Neukirchen
Matthias Book

Examiner
Thomas Welsh

Faculty of Industrial Engineering, Mechanical Engineering and Computer
Science

School of Engineering and Natural Sciences

University of Iceland

Reykjavik, September 2023

The state of cybersecurity vulnerability reporting in Iceland
(Staða tölvuöryggistilkynninga á Íslandi)

60 ECTS thesis submitted in partial fulfillment of a M.Sc. degree in Software Engineering

Faculty of Industrial Engineering, Mechanical Engineering and Computer Science
School of Engineering and Natural Sciences
University of Iceland
Dunhagi 5
107, Reykjavik Iceland

Telephone: 525 4000

Bibliographic information:

Þorsteinn Kristinn Ingólfsson (2023) *The state of cybersecurity vulnerability reporting in Iceland*, M.Sc. thesis, Faculty of Industrial Engineering, Mechanical Engineering and Computer Science, University of Iceland.

Copyright © 2023 Þorsteinn Kristinn Ingólfsson

This thesis may not be copied in any form without author permission.

Reykjavik, Iceland, September 2023

Abstract

Research and experts highlight that the level of use and knowledge of Vulnerability reporting programs (VRPs) is low and penetration testing is not done regularly. Without having knowledge of what a VRP is, a lack of a proper disclosure channel is likely. Penetration testing is a method used for securing a system, is relatively cheap, and is considered a minimum requirement for securing a system. Through two studies with questionnaires and interviews conducted with Icelandic companies, the state of this lack of use and knowledge was explored. The results show that usage of VRP is low in Icelandic companies and it is mostly due to resource limitations and lack of knowledge. Penetration testing is though relatively widely used, but can be improved. Assumingly, this is the first study which explicitly explores VRPs and attitudes in Iceland. The obtained results can be used as input for creating a VRP platform for Icelandic companies. This would raise awareness and create a safe and known disclosure channel for Iceland.

Útdráttur

Rannsóknir sýna að kunnátta á tilkynningargáttum og notkun þeirra er lág. Einnig eru skarpskyggisprófanir ekki framkvæmdar reglulega. Án kunnáttu um hvað tilkynningargáttir eru, eru háar líkur á því að ekki sé til staðar góð tilkynningarleið veikleika. Skarpskyggisprófun er prófunaraðferð notuð til að auka öryggi kerfa sem að er tiltölulega ódýr og er talin vera lágmarkskrafa þegar öryggi kerfa er skoðað. Með því að framkvæma tvær skoðanakannanir ásamt viðtölum við íslensk fyrirtæki var þessi þekkingarskortur skoðaður. Niðurstöðurnar sýna að notkun tilkynningargátta er lág á Íslandi og að það sé að mestu leiti vegna skort á fjármagni eða þekkingu. Skarpskyggisprófanir eru þó notaðar tiltölulega mikið þó hægt sé að bæta þá notkun frekar. Svo best sem vitað er þá er þetta fyrsta rannsókn á Íslandi sem að skoðar sérstaklega tilkynningargáttir og viðhorf til þeirra. Niðurstöðurnar er hægt að nota sem inntak til sköpunar á tilkynningargátt fyrir íslensk fyrirtæki. Það myndi auka meðvitund á tilkynningargáttum og búa til örugga og þekkta tilkynningarleið fyrir Ísland.

Contents

Abbreviations	xiii
Acknowledgments	xv
1. Introduction	1
1.1. Research questions	2
1.2. Approach	2
1.3. Thesis Outline	2
2. Foundations	3
2.1. Bug Bounty Programs for Cybersecurity: Practices, Issues, and Rec- ommendations	3
2.1.1. Hackers and VRP terms	3
2.1.2. Penetration testing and system scanning	4
2.1.3. Bug bounty programs	5
2.1.4. Bug bounty platform insights	7
2.2. Economic Motivations for Software Bug Bounties	10
2.3. Bug bounties and disclosure policies on state level	11
3. Related Work	13
4. Methods	19
4.1. Quantitative Research	19
4.1.1. Survey protocols	20
4.1.2. Study one	21
4.1.3. Study two	24
4.2. Qualitative Research	26
4.2.1. Interview protocols	26
4.2.2. Demographics of interview participants	27
5. Results	29
5.1. Data from Study one	29
5.1.1. Vulnerability reporting programs	29
5.1.2. Vulnerability reporting terms suggestions	35
5.1.3. Cybersecurity, scanning and disclosures	36

5.2.	Data from Study two	38
5.2.1.	Vulnerability reporting programs	39
5.2.2.	Security, scanning and disclosures	42
5.3.	Data from the interviews	45
5.3.1.	Interview one	45
5.3.2.	Interview two	46
5.3.3.	Interview three	47
6.	Discussion	49
6.1.	Discussion and conclusions	49
6.1.1.	Disclosures and Penetration testing	50
6.1.2.	Quality of disclosure reports and vulnerability disclosures that led to a fix	51
6.1.3.	Legal pursuit of vulnerability disclosures	52
6.1.4.	Type of VRP	52
6.1.5.	Best recognition for organization	53
6.1.6.	Awareness and being informed	53
6.1.7.	Is it beneficial to make use of VRPs and Penetration testing .	54
6.1.8.	Why do some organizations not identify benefits of implement- ing a VRP	55
6.1.9.	Best known VRP platforms	55
6.1.10.	Training, assessments and scanning	55
6.2.	Most important findings	57
6.2.1.	The state of Vulnerability Reporting in Iceland	57
6.2.2.	Barriers that affect the use of VRPs	57
6.2.3.	The use of penetration testing and system scanning used Iceland	59
6.2.4.	Other findings	59
6.3.	Limitations of this thesis	59
6.3.1.	Small size of data-set	59
6.3.2.	Selection method of participants may lead to bias	60
6.3.3.	Distribution	60
6.3.4.	Why were not more interviews performed	60
6.3.5.	Questionnaires	60
7.	Summary and Outlook	63
7.1.	Summary	63
7.2.	Outlook	64
	References	67
A.	Appendix	71
A.1.	Study one questionnaire	72
A.2.	Study one interview script	87
A.3.	Study two questionnaire	92

List of Figures

2.1. Google Bug Hunters Bug bounty program (BBP)	7
2.2. Comparing Privately and Socially Optimal Care	10
2.3. Division of Care by Equi-Marginal Principle	11
3.1. The five pillars from the Global Cybersecurity Index 2020	15
3.2. Evaluation of Iceland from the Global Cybersecurity Index 2020 . . .	16
3.3. Overall representation of the cybersecurity capacity in the Republic of Iceland	17
4.1. Study one: Size of company (number of employees)	22
4.2. Study one: Role inside of company (job title)	23
4.3. Study one: Organizations main focus	23
4.4. Study two: Size of company (number of employees)	25
4.5. Study two: Role inside of company (job title)	25
4.6. Study two: Organizations Main Focus	26
5.1. Study one: Questions for participants that had a VRP	30
5.2. Study one: Questions for those that answered as not having a VRP.	32
5.3. Study one: Awareness around VRPs	33
5.4. Study one: VRP beneficial	34
5.5. Study one: Awareness Of Programs	35
5.6. Study one: Best recognition for company with VRP	35
5.7. Study one: Has Received Disclosures	37
5.8. Study two: VRP program preference	39
5.9. Study two: Best recognition for organizations with a VRP	39
5.10. Study two: The beneficiality of making use of VRPs.	40
5.11. Study two: Why do organizations not identify benefits of implement- ing a VRP?	40
5.12. Study two: Best known VRP platforms	41
5.13. Study two: Interest in implementing VRP and other considerations .	41
5.14. Study two: Is penetration testing more beneficial?	42
5.15. Study two: Received disclosures in the last 3 years	43
5.16. Study two: Training, assessments and scanning	44
5.17. Study two: Questions on awareness and information.	44

List of Tables

5.1. Study one: Aggregated results from questions around interest in VRPs.	31
5.2. Study one: Suggestions from participants on VRP terms.	36
5.3. Study one: Results from questions on application security assessments, scanning and more.	37
5.4. Study two: Results from questions on received disclosures. The rows show the questions and the columns show the answers, counted in number of answers.	43

Abbreviations

BBP	Bug bounty program
CERT	Computer Emergency Response Team
DEP	Digital Europe Programme
DoD	Department of Defense
GDPR	General Data Protection Regulation
ICEDEF	Defend Iceland
ITU	International Telecommunication Union
NCC-IS	National Coordination Centre Iceland
NTIA	National Telecommunications and Information Administration
VRP	Vulnerability reporting program

Acknowledgments

First and foremost I want to thank my supervisors, Gerardo Reynaga, Helmut Neukirchen, Matthias Book, who showed me how to create this research and supported this research all the way to the finish line. I also want to thank Theódór Gíslason who acted like a further supervisor in this thesis and is included among them when “supervisors” are mentioned in these acknowledgments as well as later in this thesis. I want to thank my supervisors for their countless reviews and meetings over scripts and results, this thesis would not have been possible without their valuable counsel. I thank my friends and family for their support as without them, I would not have found the energy and enthusiasm to finish this project that is my master’s thesis. I want to thank those two that inspired the initial idea for my thesis, Gerardo Reynaga and Theódór Gíslason. I also want to thank the man who brought me in contact with these fine men, Gregory Falco. Furthermore, I want to thank the examiner of this thesis, Thomas Welsh, for taking the time for reviewing it and for his good insights. Lastly I want to thank Larry Leibrock for inspiration through his courses in cybersecurity.

1. Introduction

Cyberthreats are increasing in the world [7], and Iceland is no exception from cyber threats and needs to strengthen its capabilities to combat cyberattacks and minimize damage [10]. With an ever-changing environment of cyberattacks and defense comes the need for solutions in cybersecurity that are cheap, scalable and makes the information system as robust as possible.

Iceland ranks number 58 with a score 79.81 in the *Global Cybersecurity Index 2020* [13] of the International Telecommunication Union (ITU). In the evaluation, the category in which it was most lacking was capacity development (training, education and awareness campaigns) [13].

In the *Cybersecurity Capacity Review of the Republic of Iceland* performed in 2017 by the “Global Cyber Security Capacity Centre at University of Oxford, at the request of the Ministry of Transport and Local Government in Iceland” [5], the results were similar. The category that got the worst grade was cybersecurity education, training and skills. Three other categories out of five in the review got only slightly better grades while the category legal and regulatory framework got a considerably better grade. Within the category of standards, organizations and technology, the sub categories software quality, cybersecurity marketplace and responsible disclosure were among the ones that scored lowest in the review. This indicates poor software quality in Iceland which makes code susceptible to bugs that can be utilized to brake into systems.

To improve on software quality, the best way is to follow better software development processes, but that does not fix software that is already on the market. To fix software already on the market, bugs need to be found and patched. One way of finding bugs is to get disclosures about vulnerabilities. Therefore, to facilitate an increase in software quality, responsible disclosures can be improved upon. To increase the number of vulnerability disclosures, a Vulnerability reporting programs (VRPs) can be used to make the act of disclosing easier and safer for cybersecurity professionals [5]. Other methods of increasing quality in software via finding bugs are for example system scanning and penetration testing.

1.1. Research questions

This thesis seeks to answer the following questions:

1. What is the state of Vulnerability reporting program (VRP) in Iceland?
2. What barriers affect the use of VRPs?
3. How commonly are penetration testing and system scanning used in Iceland?

1.2. Approach

To answer these questions, surveying was performed on cybersecurity practices and vulnerability reporting in Iceland. To do this, two different questionnaires were created in separate studies, these studies will be called *Study one* and *Study two*. The first questionnaire, which was part of Study one was longer and targeted a focus group of upper management. The second questionnaire, which was part of Study two was shorter and focused on general IT professionals. Furthermore, interviews were taken with a few willing participants who took part in Study one. The data was then processed to obtain anonymous summaries. The data from these two studies was then analysed and discussed.

1.3. Thesis Outline

Following this introduction, Chapter 2 covers foundations by explaining cybersecurity terms and concepts that are used in the thesis. Related work is reviewed in Chapter 3. After that Chapter 4 outlines the research methods used in this thesis. Chapter 5 provides the data obtained in the two questionnaires along with the interviews by summarizing them through text, figures and tables. This data is then discussed in Chapter 6 and conclusions are drawn from the obtained data that is in addition compared with known data from related work. The chapter 7 concludes this thesis with a summary and an outlook. Finally, Appendix A provides the questions from the two questionnaires of the studies along with the interview script from the interviews in Study one.

2. Foundations

This chapter provides information on the Vulnerability reporting programs and Bug bounty programs and related terms used in this thesis. Furthermore, economic motivations for Bug bounty programs and disclosure policies on state level are presented.

2.1. Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations

This section introduces Bug bounty programs (BBPs) and different uses for them. It will also cover hacking terms used in this thesis as well as describe scanning and penetration testing.

2.1.1. Hackers and VRP terms

In this thesis, a few different terms are used for *Vulnerability reporting programs (VRPs)*. One of those terms are *vulnerability disclosure programs (VDPs)*, which is a synonym for VRP. Another term that is used interchangeably in the questionnaires with Vulnerability reporting program (VRP) is *vulnerability reward program*, which is another term for a BBP. A BBP is as mentioned below a type of VRP that pays out bounties.

The terms *black hat*, *white hat* and *grey hat hackers* will also be used in this thesis. A white hat hacker is someone who non maliciously breaks into systems for, for example testing their own security or under a contract with a security minded company. Through this, white hat hackers play an important role in securing software systems. A grey hat hacker is in between a white hat hacker and black hat hacker. Someone who hacks illegally, without permission but not maliciously. They look for vulnerabilities without being asked to do so and ask for a fee for found vulnerabilities. They also disclose the vulnerability if the organization does not resolve it in a timely manner. Black hat hackers, also called cybercriminals, use their skill in hacking to find vulnerabilities and exploit them, for example through selling them

2. Foundations

on the black market. This kind of hackers can be backed by governments, terrorists or simply be individuals who hack maliciously. Black hat hackers can for example hack because of grudges or simply for money [23].

Other terms that will be commonly used in this thesis for those that hack into systems are *researcher*, *cybersecurity researcher* and *cybersecurity professional*.

2.1.2. Penetration testing and system scanning

The act of *cyber scanning* is to probe networks or services for vulnerabilities or ways of infiltration [4]. Other terms used for describing this act, that will be used in this thesis, is *system scanning* or just *scanning*.

Penetration testing is a cybersecurity testing method where an information system is attacked to test the effectiveness of the system's cybersecurity. Penetration testing is performed with allowance from the company or organization that owns the information system, in fact it is often performed by the company itself or by hired cybersecurity experts. Penetration testing is used by many companies before shipping a new product or after major updates [3].

Penetration testing can be divided into conventional and unconventional penetration testing. Conventional penetration testing does not focus on automation and uses more manual methods. It focuses on modifying the system to deal with cyberattacks that are already known to avoid loss and damage from attacks. Conventional methods are effective but not efficient because of their manual nature. Because of the growing cyberspace, the conventional penetration methods have become expensive as the effort needed grows with it. Therefore, the automation of the unconventional methods become more enticing, while it is not more effective it is more efficient. While unconventional penetration testing performs the same steps to test the system, instead of the manual intensive tasks of writing scripts to emulate attacks, unconventional penetration testing uses autonomous tools that need little input from the user to perform the emulated attacks. Essentially the difference between these two methods of penetration testing is using newer methods to perform the same task of simulating attacks. Using new autonomous tools helps to increase the efficiency of the penetration testing. Another problem of penetration testing to address is that if the tests are not updated according to new attack methods used by malicious black hat hackers, they won't help properly securing the system. The same applies if the penetration testing is performed with restrictions, for example if the testing is performed only on certain parts of a system. How much freedom penetration testers get in testing systems can therefore have a big effect on the coverage of cybersecurity in systems. Malicious black hat hackers are going to use every method possible, so if the same methods have not been used in testing the

system, there is an increased likelihood of vulnerabilities to be found using those methods [3].

Scanning a system is also good to perform regularly, though unless considerable work is put into updating those scans and adding coverage by a very competent cybersecurity team, there won't be an increased cybersecurity coverage of the system. The reason for that is that running the same tests repeatedly generally deliver the same results and don't give additional information. That is why it is good to not only perform scanning but also penetration testing and try to let the cybersecurity researchers that perform it room to use those methods that they deem necessary. The same applies though to penetration testing as if the same methods or scripts are repeatedly used to penetration test a system, not much additional information is gathered compared to if new and different methods were used each time. The variety of methods that the cybersecurity researchers use is also one of the strengths of bug bounties as all kind of different individuals will try to penetrate the system.

Willingness to penetration test an information system in its entirety with any tool available is though not enough for an organization to be secure. It takes a lot of effort to try to test an information system in such an extensive way, and it is also hard to find cybersecurity experts to perform tests using all of these different kinds of penetration methods. Penetration testing performed by a limited number of individuals does not necessarily cover all different methods of penetration testing and getting into a system [3]. One way to cover this ever broadening spectrum of methods of penetration testing is using a BBP in addition to the more traditional penetration testing. Bug bounty programs can help cover the broad range of penetration methods better, as there individuals with a lot of different specializations are allowed to try and find a way into the system [17].

Information security assessments are processes to determine how well something, for example a systems or networks, meets security objectives. These assessments can be achieved through testing, exams and interviewing. Reviews of if documents are compliant with standards can as an example be a part of these processes. The term *application security assessment* will be used as another term for an Information security assessment [24].

2.1.3. Bug bounty programs

The use of *Bug bounty programs (BBPs)* is becoming increasingly common, and more and more companies are utilizing it as a way of securing their software. BBP is a decentralized version of cybersecurity testing where cybersecurity professionals can legally hack the software of companies as long as they follow the rules the companies set, report any vulnerabilities they find and later get paid for those vulnerabilities

2. Foundations

that are accepted as valid by the company. This has some things in common to the description of penetration testing. In fact, these two ways of testing software partly test the same things though through a decentralized structure in the case of BBPs [17].

There are different types of BBPs. *Institutional programs* are hosted by the software vendors themselves as well as setting policies and compensation. A *BBP platform* is where a separate entity hosts programs from many companies at the same time, the reward is decided by the companies themselves. *Private intermediary programs* are those entities that buy vulnerabilities from researchers and resell them to the companies, these program tend to have higher rewards compared to the other types. These private intermediary programs will be talked about as private BBPs in this thesis. Further than that, there are also different variants of these types of bug bounties. That is *invite-only programs*, *fuzzing competitions*, *open-ended BBPs* and *short-time-frame competitions*. Bug bounties can be used in different phases of software development. For use of BBP in the development phase, it is recommended to use a private fuzzing competition. In the beta phase as well as the product launch, it is good to host an invite-only BBP. In the postrelease phase it is advised to have an open-ended BBP, invite-only BBP or fuzzing competitions.

Many large organizations use BBPs, such as the U.S. Department of Defense (DoD), Netflix, Microsoft, Apache, Facebook, or Google. [17]. An example web page is shown in Figure 2.1. Examples for company independent BBPs are HackerOne¹ and BugCrowd².

Though BBP platforms make setting up BBPs simpler, there are many things to keep in mind. For example, it is recommended to include cybersecurity researchers through testing in the prebeta and beta phases as then the cost of fixing a bug is lower than later in the development cycle [18]. It is also a good practice to tie the size of bounties to the quality of the report along with the severity of it. Invite-only BBPs generally have higher compensation as they draw in cybersecurity researchers of high caliber. Ensuring the cybersecurity researchers that no legal action will be taken against them for reporting vulnerabilities is of great importance for attracting cybersecurity talent to the program. It is important to outline the scope of the BBP and what is not in scope so that the cybersecurity professionals know what they should search for, this can also be used to set the focus of the BBP to the type of vulnerabilities that the company needs information on the most. It is necessary to have bounties that can compete with bounties in other BBPs. Giving researchers recognition for their contributions is important as well as nurturing a talent pool, for example through invitations to invite-only programs [17].

¹<https://www.hackerone.com>

²<https://www.bugcrowd.com>

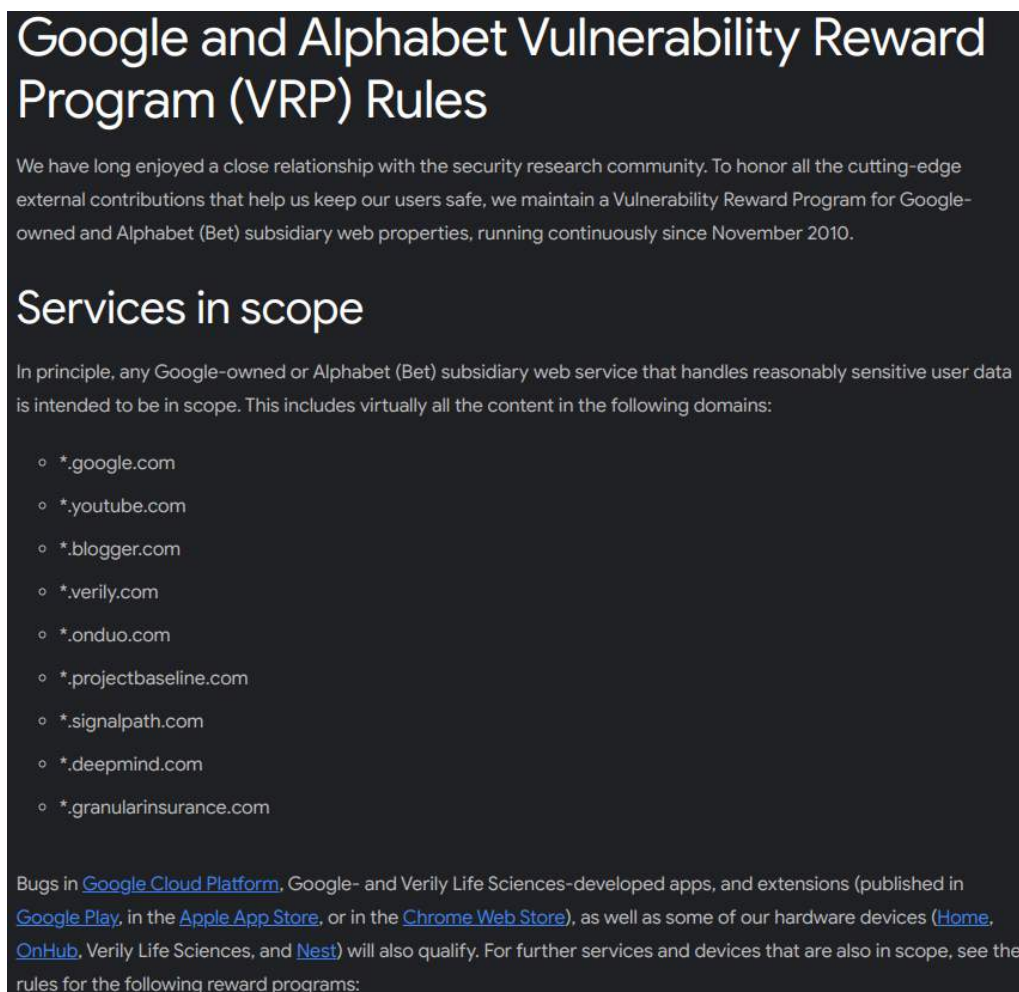


Figure 2.1: Google Bug Hunters BBP, Figure from Google, *Google and Alphabet Vulnerability Reward Program (VRP) Rules* [9]

Organizations that can add a file `security.txt` to their website. Such a file is a text file that shows the vulnerability disclosure practices in a company and should be placed in a known location [8].

2.1.4. Bug bounty platform insights

In the 2021 hacker report [12] from the BBP platform *HackerOne*, a remarkable increase in the number of hackers using the platform could be noted. Between the years 2020 and 2021, there was an 63% increase in the number of hackers submitting vulnerabilities. In the 2021 hacker report, it was also reported that the number of registered hackers had doubled to over one million since 2019. In 2022, hackers earned \$40 million on the platform. Just over half (55%) of the hackers on HackerOne

2. Foundations

in 2022 were under 25 years old and 82% of hackers were hacking part-time. When asked why they hack, 85% of the hackers answered as hacking to learn, 76% to make money, 65% to have fun, 62% to advance their career and 47% to protect and defend business and individuals. Fifty percent of hackers had chosen to not disclose a bug they had found in 2021. There were a few reasons for that, 27% report the reason being a lack of a channel to disclose through, 27% because of the company previously having been unresponsive or difficult, and 19% because no bounty was offered. It can be seen that having a clear way of disclosing as well as a good process around it can make it more likely that hackers report a bug if they find one in an organizations systems [12].

In the Hacker-Powered Security Report 2022 [11] from HackerOne, 92% of ethical hackers say that they can find vulnerabilities that the cybersecurity scanning can not. Perhaps that will change in the future with quantum technology, but for now at least human creativity is an important part in finding vulnerabilities in systems. Most hackers (85%) think that companies should be more transparent around disclosures. Fifty percent of hackers said that they had at some point chosen not to disclose a vulnerability in 2022, just like in 2021. In 2022, 42% reported the organization not having a disclosure program as a reason and 12% reported threatening legal language as a reason for not reporting [11].

On *Bugcrowd's* website, it can be seen that 75% of hackers on the platform report non-financial factors as their main motivators towards hacking. Furthermore, 87% of hackers on the platform think that it is more important to report a critical vulnerability than to try to make money from it [2].

As can be seen from a third of hackers finding that the biggest road block to them succeeding when working with an organization being a lack of scope, it is very important to not limit hackers too much. Limitations of scope tend to keep hackers away from finding vulnerabilities that have a big impact. It is therefore recommended keeping in mind that limiting scope reduces the effectiveness of hackers and the service they provide.

As vulnerabilities that are reported need to be reviewed, at least having an individual to review vulnerability reports would perhaps be the minimum of what organizations need to do. If it is given that organizations should at least be able to review reports of vulnerabilities responsibly, then the only obvious cost factor of having a VRP is simply posting the rules that hackers need to abide to as well as how to disclose to the organization on their website. That is if the VRP does not include monetary rewards. Most hackers (75% according to [2]) hack for non-monetary reasons and 87% of hackers find reporting a critical vulnerability more important than making money off of it [2]. That shows the importance of having a way of reporting vulnerabilities, such as a simple VRP on their websites that does not promise any monetary reward but outlines what is OK to do when penetration testing their system and how

2.1. Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations

vulnerabilities can be reported to them. BBPs have higher costs than VRPs because of the bounties paid out, though that increases the interest of security experts of penetration testing an organization's system [2].

VRPs can be hosted in many ways, for example as a self-hosted VRP, self-hosted BBP or through a BBP platform. There are though different kinds of BBPs for different use cases. As an example for systems that are sensitive in nature and host sensitive data, an invite-only bug bounty might be a good idea. This way the scope of the simulated attacks can be better controlled, and the organization can choose to only invite a certain number of trusted cybersecurity researchers to take part in the program. Invite-only bug bounties do though tend to have higher bounties as they are meant to attract cybersecurity researchers that are good at what they do and can be trusted. Something that can bring the cost of fixing a bug is to fix it early in the development cycle. This is something that VRPs and BBPs can be used for also. During development of software, a recommended type of BBP to use would be private fuzzing competitions. During the beta phase of software development, invite-only BBPs can be hosted to find and address bugs early [17].

There are though not only different types of VRPs, but also different motivations for hacking and reporting vulnerabilities. When asked why they hack in the report Inside the mind of a hacker 2023 from Bugcrowd, 24% of hackers say that financial gain is the reason. The rest of the hackers hack for non-financial reasons. As an example 28% of hackers hack for personal development, 14% for excitement and 6% for the greater good. Hackers also do not choose a VRP only by which one has the biggest monetary reward. There are though many reasons stated in the report for why they choose a specific program. Many choose monetary reasons such as higher value per finding (44%) or fast time to payment (50%), but there are more reasons that are not directly monetary in nature. In fact the most common reason (61%) is because of a responsive team and other than that, new technologies (52%) is also a common reason along with a breadth of scope (50%) and familiar technologies (44%) [2]. In the 2022 hacker powered cybersecurity report from HackerOne, the most popular (65%) reason to choose a program to hack was the bounty. After that liking the brand (38%) and having a challenge and opportunity to learn (40%) were second and third most popular reasons. Other common reasons were that they use the company's product (27%), a varied scope (36%), they received an invitation to a private program (34%), fast resolution time (28%) and fast bounty time (32%) [11].

2.2. Economic Motivations for Software Bug Bounties

While VRPs and BBPs cost money, there are economic motivations for these. Figure 2.2 depicts the connection between privately and socially optimal care. Because software developers are currently shielded from liability from bugs in products, they have an incentive to let many bugs go unpatched instead of fixing them. For the society, it is optimal to have the most care to find and fix bugs in software. In the triangle $ab0$ in Figure 2.2, the social surplus can be seen which can be captured by a successful policy. A successful policy in this case would be one that increases the care to find and fix bugs in software. One way to get developers to put more care into finding and fixing bugs is making them more liable for harm done by their software because of bugs. To seek to cover the liability, the developers can outsource bug finding through bug bounties. Though in that way, bug bounties can work as a patch to a wound as the developers may put less effort into writing safe software to begin with and use bug bounties to patch the buggy software after it is released in favor of not slowing down software development [25].

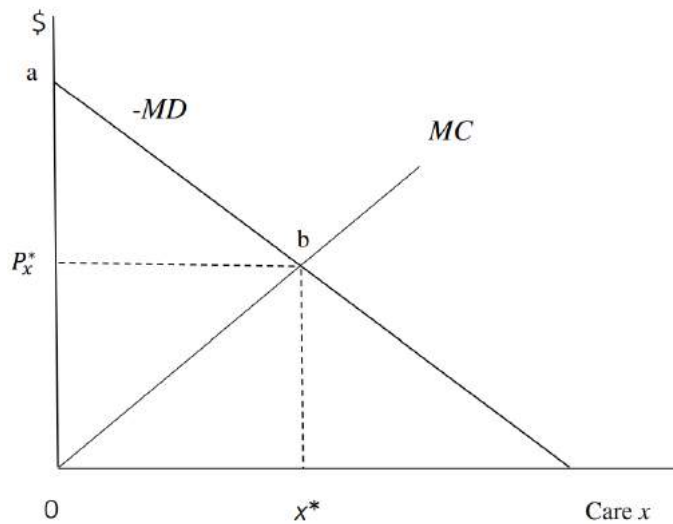


Figure 2.2: Comparing Privately and Socially Optimal Care x , Figure from Christopher Sprague and Jeffrey Wagner, *Economic Motivations for Software Bug Bounties* [25]

Figure 2.3 shows the relationship of expended care between developers and bug hunters. To the far right, developers expend all the care to find bugs. To the far left, all the care is expended by the bug hunters. The marginal cost lines show the marginal cost for the developers (MC_d) and the bug hunters (MC_h). The level of care in the space between the far right and to the point where the marginal lines intersect (X_d), are levels where the developer will stand to gain from paying the bug

hunter to find the bugs for them [25].

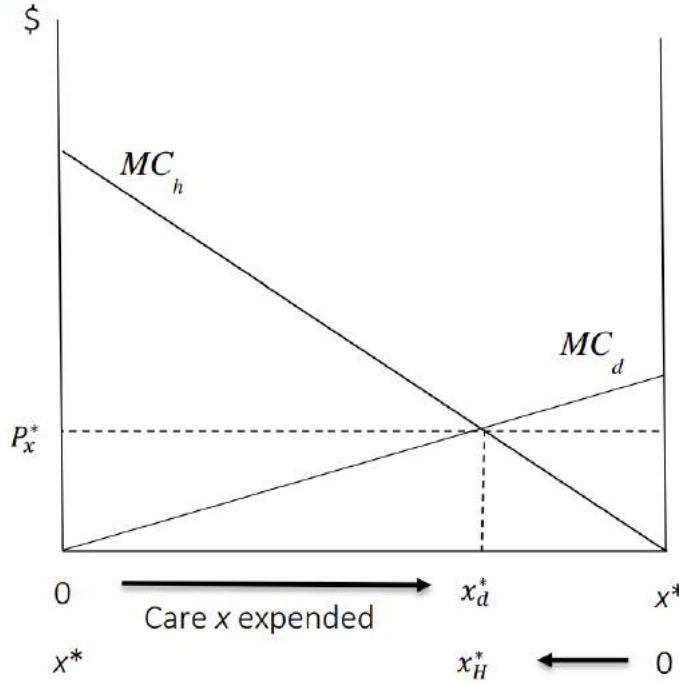


Figure 2.3: Division of Care by Equi-Marginal Principle, Figure from Christopher Sprague and Jeffrey Wagner, *Economic Motivations for Software Bug Bounties* [25]

2.3. Bug bounties and disclosure policies on state level

A few states have shown interest in disclosure policies and programs. The Netherlands was first at creating a disclosure policy, which acts as a guideline even if it is not a law [14]. Latvia took it a step further and created regulations around the responsible vulnerability disclosure process [14]. In addition, France is already implementing a disclosure policy that will protect cybersecurity researchers [6]. The United States authorities along with the United Kingdom have shown interest in creating a responsible disclosure policy. As an example of interest, U.S. assistant Attorney General Leslie Caldwell described the “Hack the Pentagon” BBP project as laudable. This project was created by the U.S. DoD in cooperation with the U.S. Department of Justice’s Criminal Division. Not only countries are creating vulnerability disclosure policies and bug bounties, many companies have also starting doing so. An example of larger companies that have created vulnerability disclosure policies or bug bounties are Microsoft, Uber, IBM, Facebook and Google [14].

2. Foundations

To create a disclosure policy, clear rules should be laid out. What can and cannot be done should be clear, for example what methods can be used and what kind of vulnerabilities can be reported. It needs to be clear where cybersecurity researchers should report vulnerabilities to, for example to a BBP, VRP or a national Computer Emergency Response Team (CERT). Giving out monetary prizes in BBPs can motivate cybersecurity researchers to report vulnerabilities [14].

Creating laws around disclosures is not as straight forward as one could think. The legal frameworks between countries are different, and it will therefore not be as hard in every country. One thing to keep in mind is to make sure that the new law does not make research into finding cybersecurity flaws illegal. If that happens, it would make it much harder to involve independent cybersecurity researchers in building cybersecurity in cooperation with the government and organizations. Another problem is not to make the law so inclusive that the act of reporting does not rid a reporter of all responsibility. If reporters of vulnerabilities can legally rid themselves of responsibility by reporting the vulnerability, then a malicious hacker could hack into a system, steal data, sell the data and then make sure they are not sued by reporting the vulnerability afterwards. The laws therefore need to be well thought out and written so that it protects both reporters that reports in a way that is generally thought of as inside the law as well as the country and organizations [14].

There are different ways of disclosing vulnerabilities. One important one is through full disclosures, which is when all information about a vulnerability is shared to the public without the vendors consent. This can lead to IT cybersecurity risks. A good thing about full disclosures is that the public scrutiny that follows can put pressure on organizations to fix these vulnerabilities. Another point that advocates of full disclosure often mention is that it is ethically correct to let the public know of vulnerabilities so that the users of software can protect themselves. A downside of full disclosure is that disclosing as much information as possible increases the risk for everyone. Another important kind of disclosure is responsible disclosures. Responsible disclosure policies are policies of how to disclose vulnerabilities responsibly and encourages independent grey hat researchers in the disclosure process to disclose vulnerabilities. They generally include discovery, reporting, response from the vendor and publishing of limited information. These policies can strengthen the cooperation between vendors and cybersecurity researchers along with giving researchers guidelines of how they should go about finding, reporting and publishing vulnerabilities. Responsible disclosure policies are considered as effective in disclosing a dangerous kind of vulnerabilities called “zero-day” exploits [14].

3. Related Work

This chapter covers publications related to the research questions underlying this thesis.

Ita Ryan, Utz Roedig and Klaas-Jan Stol [21] performed a questionnaire on security practices and security culture along with investigating their correlation. The responses to this questionnaire came from 59 different countries, the highest number of responses coming from the United States. The total number of responses was 1100. The result of the study was that there was not a strong correlation between organizations having good security practices and having a good security culture. Even if security is high priority in the organization, the security culture can be unfavorable and only the minimum is done for security compliance. The respondents with the lowest grade in software security practices spent less than half an hour a week on security activities while the organizations with the highest software security practice grade still spent only less than two hours a week on security activities on average. The results from the questionnaire also stated that 31.7% of participants in the survey answered that external penetration testers were used to identify security problems. These percentages for the use of penetration testers were though not provided per country, but rather only as an average of results from all the countries [21].

Tamara Lopez et al. [16] performed a multi sited ethnographic study in the UK over a 2.5 year period that sought to answer where security can be found in normal development environments and what security practices non-specialist developers have. The participants were 23 developers from two different companies. The results of the study was that developers respond to security needs in situations within the dimensions of common development practice. How a developer responds to these needs is influenced by the task, local problems and the developer's orientation to the situation. Developers generally think that following a companies security policies makes sense and associate code security with writing good software. Lastly the attitudes and priorities of companies and clients are reflected on to decisions that impact security in code [16].

Irum Rauf et al. [20] conducted a study with 124 freelance developers, which were mostly from Asia. The study consisted of code review tasks with open-ended responses that the researchers used to assessment the engagement of developers with

3. Related Work

code, as well as psychological questions to assess their attitudes. They conducted this study to understand how social priming influences the security engagement of developers with code and how they attend to security in code. The results of the study could not conclude if social priming affected the participant's engagement with security in code. Forty four percent of participants did though talk explicitly about security during engagement with code when they had not been socially primed to security. When security requirements were not specified, developers in the study attended to security according to their own security views instead of security expected by software owners. Social considerations towards other developers and the wider good were though also key motivation of the developer's security practices [20].

The U.S. National Telecommunications and Information Administration (NTIA) Awareness and Adoptions Group [19] performed two surveys, one with security researchers (414 responses) and the other with software vendors (285 responses). The questionnaires looked into the past or current behavior around responding or reporting of vulnerabilities along with working processes and possible improvements to them. The results from the researcher survey was that most (92%) cybersecurity researchers take part in a coordinated vulnerability disclosure. Cybersecurity researchers also generally publicly disclose vulnerabilities only after poor communications or other frustrations. The threat of legal action is a reason for not disclosing for 60% of cybersecurity researchers. Lastly, 70% of researchers expect good communications but only 15% expect bounty. The results from the vendor survey was that most (76%) mature technology providers develop vulnerability handling procedures internally, few look at international standards of how other organizations implement this. Few (one in three) organizations stated that their suppliers had their own vulnerability handling procedures or required them to do so. The reason that mature vendors had disclosure policy was reported as being because of a sense of corporate responsibility or their customers wanting it [19].

The United Nations specialized agency International Telecommunication Union (ITU) performed a survey [13] that asked the union member states questions covering five pillars of cybersecurity. Those pillars are legal, technical, organizational, capacity development and cooperative measures. The definitions of these five pillars can be seen in Figure 3.1.



	Legal		
Measuring the laws and regulations on cyber-crime and cybersecurity	167	Countries with some form of cybersecurity legislation	
	133	Data Protection Regulations	
	97	Critical Infrastructure regulations	
	Technical		
Measuring the implementation of technical capabilities through national and sector-specific agencies	131	Active CIRTs	
	104	Engaged in a regional CIRT	
	101	Child Online Protection Reporting mechanisms	
	Organizational		
Measuring the national strategies and organizations implementing cybersecurity	127	National Cybersecurity Strategies	
	136	Cybersecurity Agencies	
	86	Child Online Protection strategies and initiatives reported	
	Capacity development		
Measuring awareness campaigns, training, education, and incentives for cybersecurity capacity development	142	Countries conduct cyber-awareness initiatives	
	94	Countries with cybersecurity R&D programs	
	98	Countries reported having national cybersecurity industries	
	Cooperation		
Measuring partnerships between agencies, firms, and countries	166	Countries engaged in cybersecurity Public-Private Partnerships	
	90	Countries with cybersecurity bilateral agreements	
	112	Countries with cybersecurity multilateral agreements	

Figure 3.1: Five pillars of cybersecurity, Figure from the International Telecommunication Union, *Global Cybersecurity Index 2020* [13]

3. Related Work

In the survey, which was performed in 2020, questionnaires got returned from 150 member states. As can be seen in Figure 3.2, Iceland scored the lowest in capacity development. The scores for some other categories are also not as good as they could be, for example in the technical measures and cooperative measures. It is though unclear in which category of the five pillars VRP would fall into. The overall grade of Iceland is 79.81 and ranked 58th in the rankings. In comparison, Estonia ranked 3rd with a score of 99.48, Norway ranked 17th with a score of 96.89 and Denmark ranked 32nd with a score of 92.6. The score of Iceland is therefore comparatively low compared to these neighboring countries [13].

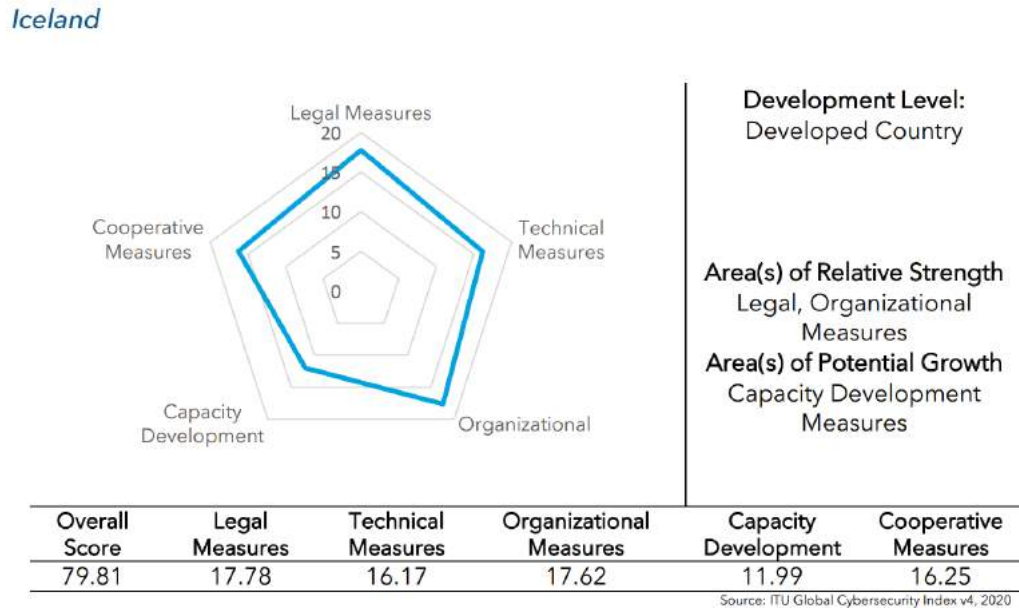


Figure 3.2: Evaluation of Iceland, Figure from the International Telecommunication Union, *Global Cybersecurity Index 2020* [13]

The Global Cyber Security Capacity Centre at Oxford University [5] did at the request of the Ministry of Transport and Local Government in Iceland perform a review of the maturity of the cybersecurity capacity of Iceland. A series of consultations were performed with staff from the following sectors: government departments and ministries, legislators and policy owners, criminal justice, law enforcement, academia, and private and financial sectors. These consultations involved 60 institutions and enterprises in Iceland, and focused on the five following dimensions: Policy and strategy, Culture and society, Education and training and skills, Legal and regulatory frameworks, Standards and organisations and technologies. As can be seen in Figure 3.3, Iceland got a poor grade in many parts of the review. Some exceptions to that are the sub categories for legal frameworks and national cybersecurity strategy. The subcategory for responsible disclosures, which a VRP would fall into, gets a bad grade along with the category for software quality. It is not clear in which subcategory penetration testing would fall into, but it at least falls

into the category for standards, organizations and technologies, which gets a poor overall grade [5].

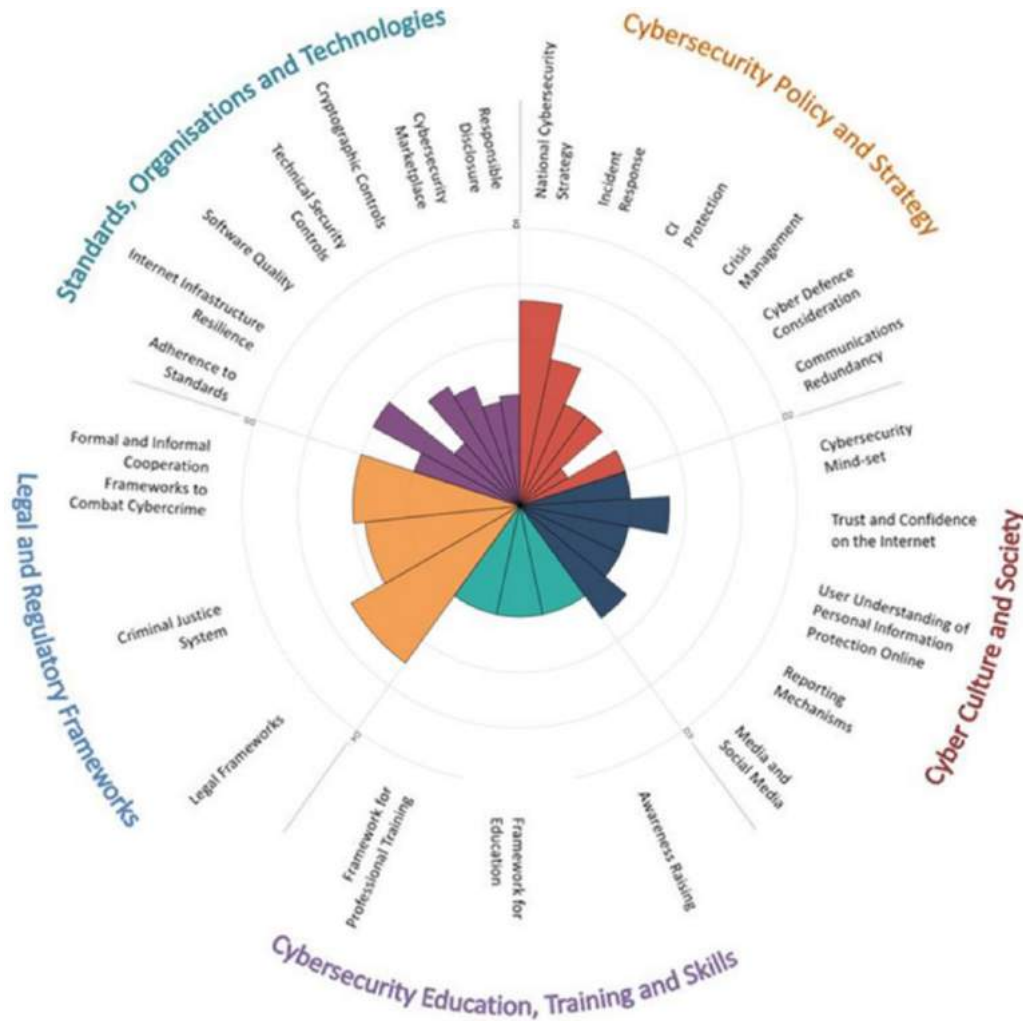


Figure 3.3: Overall representation of the cybersecurity capacity in the Republic of Iceland, Figure from the Global Cyber Security Capacity Centre, *Cybersecurity Capacity Review Republic of Iceland* [5]

Arnardóttir et al. conducted as part of their Bachelor's thesis [1] ten interviews with managers responsible for IT security at Icelandic companies. The topic of this qualitative study was to find out about the most important cybersecurity challenges and tasks that the interviewed managers face during their work. However, these interviews did not cover VRP or technical aspects such as penetration testing or security scanning [1].

4. Methods

This chapter describes the methods used in the research of this thesis and the demography of the involved participants. The results are described in Chapter 5.

For this research, a mix of quantitative and qualitative research was used. Quantitative research is based on objectivity independent of human perception and like in a one way mirror, the investigator does not influence the investigated and vice versa. In quantitative research the sample sizes are much larger than in qualitative research. What quantitative research seeks to do is measure and analyze causal relationships between variables. Ways to do that include randomization, highly structured protocols and questionnaires with a limited range of predetermined responses. The quantitative technique used here are questionnaires with predetermined responses, though in some cases allows open-ended answers [22].

Qualitative research is based on there not being one truth, but rather multiple realities and multiple truths as reality is socially constructed and constantly changing. In qualitative research, the investigator and the investigated are linked in interaction and the findings are created within the context of the situation of the inquiry. It focuses on process and meanings. Ways to do this include in-depth and focus group interviews along with participant observation as the samples are not meant to represent large populations. The sample size is small but purposeful, and here in depth interviews were taken with participants from the subset of those that took part in the quantitative questionnaires on the subject [22].

4.1. Quantitative Research

Two studies were designed along with follow-up interviews after the first study. These studies were conducted with participants in Iceland and asked employees about vulnerability reporting and cybersecurity practices inside their organizations.

4.1.1. Survey protocols

The two studies have two slightly different target groups, but follow the same general process. That process was that the online questionnaires were written in Icelandic and English, and no time limits on how long participants took to complete the questionnaires were imposed.

Study one targeted upper management and cybersecurity professionals, this was done by sending the questionnaires using the professional networks of the author of this thesis and his supervisors along with sending it to Icelandic cybersecurity and project management Facebook groups. The study was also designed with the knowledge of the upper management and cybersecurity professionals in mind and asked questions about VRP that these individuals would have a say in the implementation of. For further details on the demography of the participants in Study one, see section 4.1.2.

Study two aimed at reaching a broader group by targeting programmers and IT professionals in general without necessarily having a cybersecurity focus. This was done by using the professional networks of the author of this thesis and his supervisors along with posting to Icelandic programming, cybersecurity and management Facebook groups. As such, the questionnaire in Study two was designed with the knowledge of general IT professionals in mind as well as to gain an insight concerning their knowledge on the subject. For further details on the demography of the participants in Study two, see section 4.1.3.

The study protocols along with the questionnaires and interview script were improved in a series of reviews together with the supervisors of the project with improvement sprints in-between.

The tool that was chosen to design and deliver the questionnaire was SoSci Survey [15]. This tool was chosen as it had good branching functionality, i.e. guide the participant along different branches of questions depending on their previous answers, along with being free of charge for academic research within certain terms. The terms were that questionnaire must have no commercial background and be anonymous [15]. SoSciSurvey's General Data Protection Regulation (GDPR)-compliant cloud service was used instead of getting a license and running it on an own server setup.

To make sure that the questionnaires asked the right questions and had good wording, the questionnaires went through iterations of reviews by the group of thesis supervisors. Through improving upon the items in the feedback from the reviews, the quality of the questionnaires became steadily better.

For the questionnaire in Study two, the questionnaire from Study one was used as a base. This questionnaire was made as a shorter version of the questionnaire in Study one, to appeal to the new target group. Having a good initial base to work from, and the experience gained from reviewing the questionnaire from Study one resulted in needing only a few iterations for creating the questionnaire in Study two.

4.1.2. Study one

Study one sought to answer the questions: Have organizations been getting disclosures in the last years, whether there is any existent interest in VRPs, what barriers might be in the way of implementing such a program, and on the usage of penetration testing and security scanning (covering the research questions, see section 1.1). The questionnaire in Study one was designed to get answers to these questions.

Advertising the questionnaire

A list of individuals was compiled by the author of this thesis, the thesis supervisors and other individuals, and an email sent out to these individuals. The estimated time for finishing the questionnaire was in the email stated to be eight minutes, though that might have been an underestimate considering the time it took already to take the shorter questionnaire in Study two. Furthermore, a post was sent to the Facebook group of cybersecurity in Iceland. That group is called “Netöryggi – hópur um öryggismál veflausna”, it has 3.6 thousand members and is for posting information about and discussing cybersecurity.

In the questionnaire, respondents could at the end choose to take part in a follow-up interview and leave their contact information (name and email) either connected to their answers or without association to their answers.

Study one was available on ScoSci Survey from 28.3.2022 to 30.9.2022, it was available this long as there was an ongoing effort to get more participants. The ongoing effort did somewhat pay off as responses continued to come in during the summer. In the end, the number of total participants was 31 in Study one.

A filtering of data points used in both studies was removing those data points where participants only answered questions on the first page which consists of demographic questions. However, in Study one no participant only reached the first page in Study one, and therefore the number of data points is equal to the total number of participants.

Demographics of participants

In Figure 4.1 it can be seen that the participants are working for organizations of different sizes. The most common organization size is 101–500 employees (9 participants gave that answer). Some sort of median split is at 100 employees: the number of participants that worked at organizations with 100 or fewer employees were 11, while 16 worked at organizations with over 100 employees.

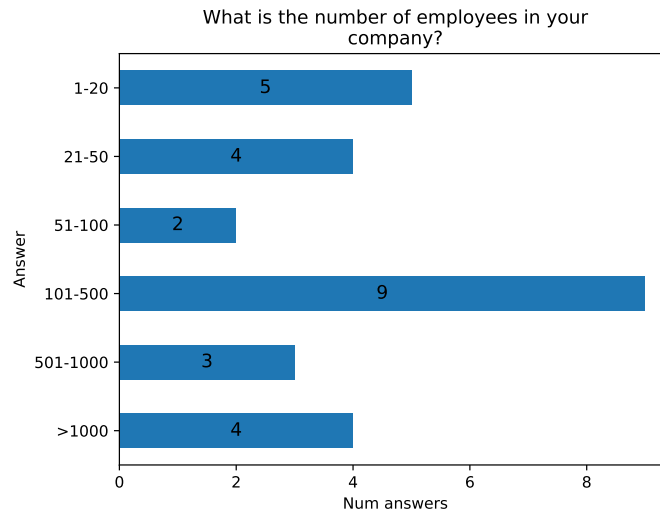


Figure 4.1: Study one: Size of company (number of employees)

Twenty (74%) participants of this questionnaire answered as being in some sort of management role as can be seen in Figure 4.2. Those who were not in management roles were in the following roles: three can be summarized as programmers and cybersecurity professionals, and four participants answered with “Other”. The “Other” field allowed participants to provide free text: from these four “Other” answers, two answered to be in management roles that did not fit the management roles provided in the available selections. With these two further management roles, the total number of management roles increases to 22 (81%).

When asked what the geographical reach of their organization was, 16 (59%) participants answered as working for organizations with national reach. Four participants answered that their organizations had European reach and seven with international reach, which makes 11 (41%) participants that work for organizations with operations reach outside of Iceland.

When asked about the age of their organization, 18 (69%) participants said they worked at organizations that are more than 16 years old. Three participants answered with younger than five years old, four answered with five to ten years old

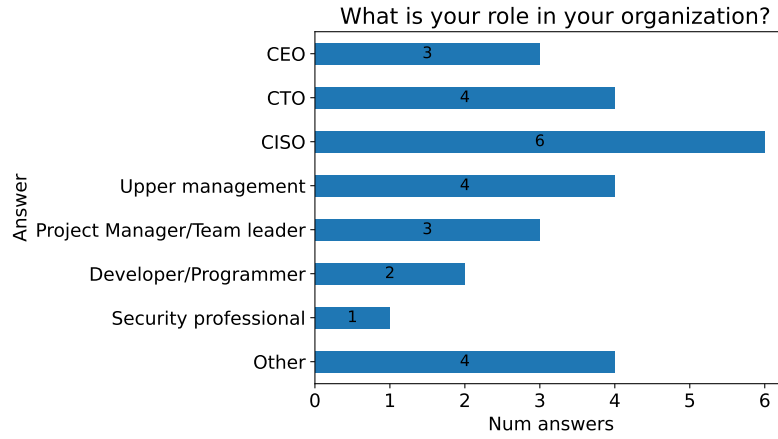


Figure 4.2: Study one: Role inside of company (job title)

and one participant answered with 11 to 15 years old. Which makes eight (31%) participants that answered as working for organizations younger than 16 years old against 18 that answered as working for organizations older than 16 years old.

As can be seen in Figure 4.3, the participants were from organizations focusing on different domains. Ten (37%) participants chose to specify the organizations' focus in the "Other" input field. From the free text field available for the "Other" selection, there were two responses as data/databases and one as scientific research. Other single instance responses were: cybersecurity, software, energy, consulting, telecommunications, managed service provider.

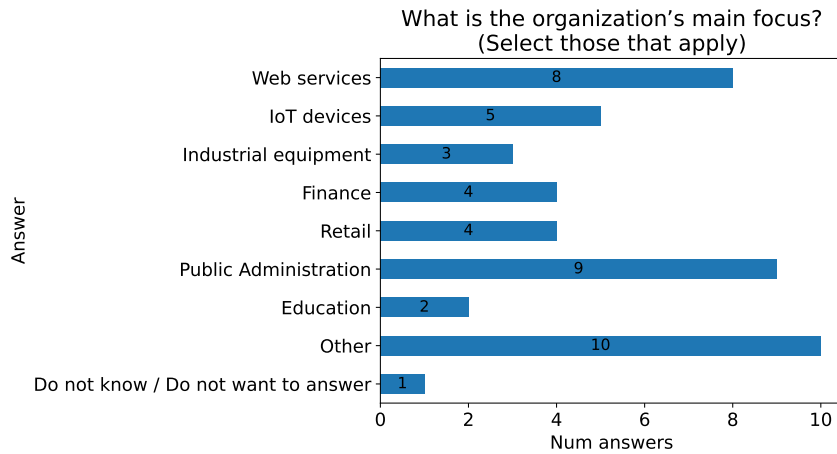


Figure 4.3: Study one: Organizations main focus

4.1.3. Study two

A few participants in Study one mentioned the questionnaire being too long after taking it, a few mentioned this in replies of an invitation email sent to them to take part and a couple through interviews. Therefore, for Study two, the aim was to shorten and simplify the questionnaire along with the informed consent text. When advertising the questionnaire, the stated time estimate for taking the questionnaire was ten minutes.

In addition, Study two aimed at a wider and more general audience of IT professionals, that along with the questionnaire being shorter resulted in more individuals participating in the questionnaire. Study two was designed to answer questions on: What IT professionals think about VRPs, how much they know about them and how the culture around VRP and cybersecurity is in their organizations. Just as in Study one, this allows to answer the research questions (see section 1.1), however with fewer questions and wider, but less focused group of participants.

Advertising the questionnaire

The questionnaire was posted on two Icelandic Facebook groups, “Forritarar á Íslandi”¹ and “Félag Tölvunarfræðinga”², that have 7.3 thousand and 1.3 thousand members respectively. The former group is a group to talk about anything around programming or programming projects. The latter group is a group for the Icelandic association of computer scientists with university education where members of the organization can communicate.

The number of total participants was 71 and after filtering, the total number of data points remaining was 59. The filtering applied was to exclude those that only reached the first page of questions, which included only demography questions (see section 4.1.3). The questionnaire was online from the 21.02.2023 to 28.04.2023.

Demographics of participants

Figure 4.4 shows that 29 (53%) participants, work at organizations with above 100 employees.

¹<https://www.facebook.com/groups/415940541830603>

²<https://www.facebook.com/groups/10760077999>

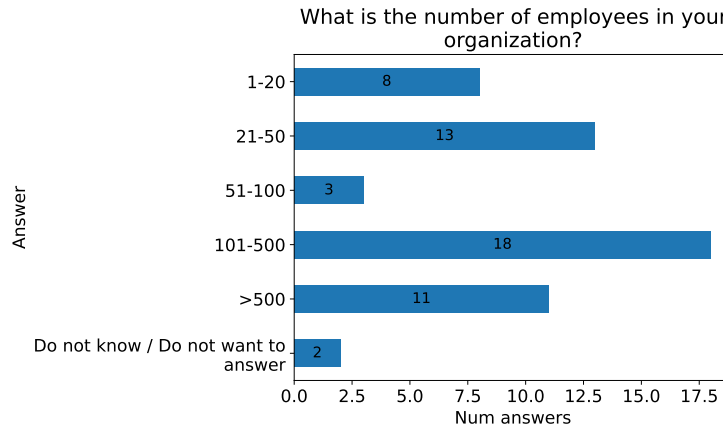


Figure 4.4: Study two: Size of company (number of employees)

In Figure 4.5 we can see that 22 (42%) of the responses are from programmers and altogether 16 (30%) from project managers/team leaders and cybersecurity professionals. This reflects the targeting in the distribution of the participants as was intended. From the “Other” field free text answers, three further participants can be classified to belong to the management category. Additionally, three answered as working in various positions around data and systems and three answered with different positions that did not fit well into one category.

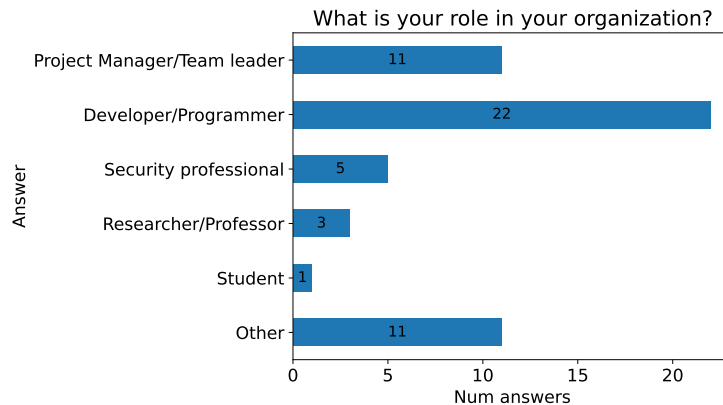


Figure 4.5: Study two: Role inside of company (job title)

When participants were asked about the geographical reach of their organization, 33 (60%) answered as having national reach, 19 (35%) with International reach and 3 (5%) with European reach.

When asked about the age of their organization, 41 (75%) participants said that they work at organizations that are 16 years old or older. Four participants answered with younger than five years old, six answered with five to ten years old and three participant answered with 11 to 15 years old. Altogether, 13 (24%) partici-

4. Methods

pants answered as working for organizations younger than 16 years. One participant answered as not knowing or not wanting to answer.

As can be seen in Figure 4.6, the domain on which organizations of the participants' focus was quite varied. Twenty one (38%) participants chose to use the “Other” input field to answer the question. Other than this “Other” field, the most common main focuses specified were finance with 14 (25%) answers, Web services with 12 (22%) answers and public administration with ten (18%) answers. From the “Other” input field, answers with these main focuses were added to summarize: four answers as data and databases, two answers as cybersecurity, two as computer games, two as software development, two as energy and two as healthcare. Five answers from the “Other” field did not fit well into any category and varied between different sectors. Those different sectors included production systems, transportation, research, infrastructure, consulting.

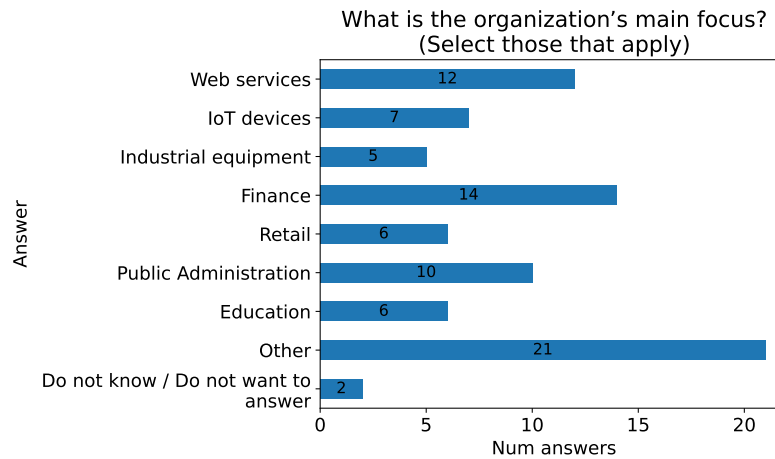


Figure 4.6: Study two: Organizations Main Focus

4.2. Qualitative Research

This section will describe what methods were used in the qualitative research in the creation of this thesis. In the online questionnaire of Study one, participants could opt to leave an email address in order to get contacted for a further interview.

4.2.1. Interview protocols

The target audience of the interviews were the participants of Study one, that means that these were also individuals mostly in higher management positions. The ques-

tions for the interviews were designed to probe further on material that had been asked about in Study one.

The script with interview questions was reviewed by the supervisors of the thesis and improved on until they were deemed of sufficient quality. The questions were designed in Icelandic and English and the estimated time for the interviews were 45 minutes. Two interviews were in person and one was performed through remote meeting software.

In the beginning of the interviews the participants were greeted and given a short introduction on the material of the interview. The participants were asked for consent for the audio of the interview to be recorded before turning on the recording device that formally started the interview. The interviewer took notes during the interview and the interviews were also audio recorded with the participants consent.

In the interviews the participants were then asked questions on the subject of VRP from the script of interview questions, including why they answered questions from the questionnaire a certain way and open-ended questions on the subject of vulnerability reporting. In the end of the interviews, the participants were asked about any further thoughts and questions as well as if they were interested in receiving a copy of the final results of the study.

4.2.2. Demographics of interview participants

Interviews were taken with three individuals who signed up for interviews in the questionnaire in Study one. All three individuals had good knowledge of VRPs and security practices. Furthermore, two out of three were in management roles revolving around security.

5. Results

The previous chapter provided information on protocols used as well as the demography of participants. This chapter provides the actual data obtained from the studies. Because the thesis author promised to only publish summaries of answers in a disclaimer in both the questionnaires and in the interviews, there will only be summarized data. That means that answers from individuals will not be provided in this thesis or as part of further research using the data, and no transcripts of interviews will be presented. The data provided in this chapter is then further analysed and discussed in Chapter 6.

5.1. Data from Study one

In this section the results from Study one are provided. As explained in section 4.1.2, the participants in Study one were mostly individuals with a background in management.

The number of total participants in this study was 31 in Study one and as already mentioned in section 4.1.2, no one was filtered out, so the number of total data points used was also 31.

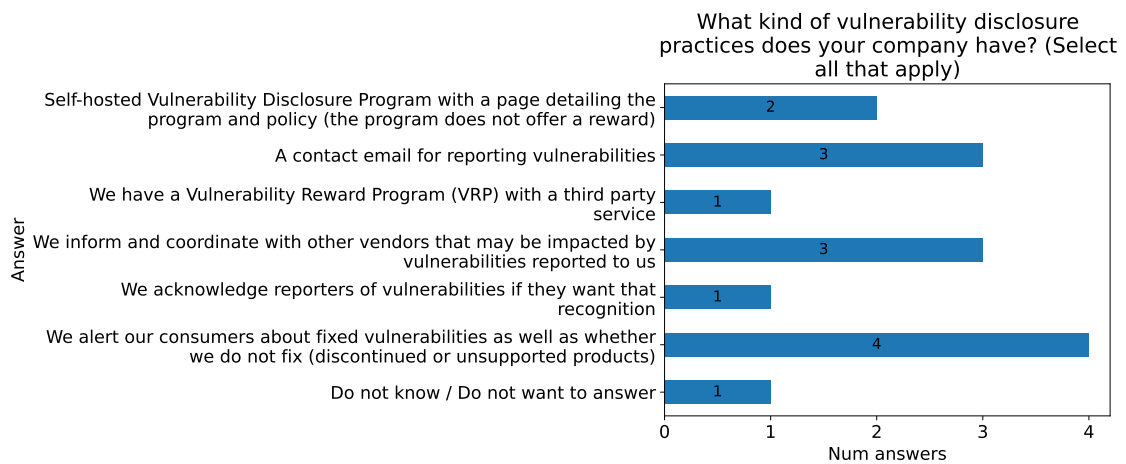
5.1.1. Vulnerability reporting programs

When participants were asked if their organizations had a vulnerability disclosure program, six (27%) answered “yes” and 16 (73%) answered “no”. Depending on whether a participant answered as their organizations having a VRP or not, different follow-up questions were asked. These are described in the following subsections. Participants were also asked about other practices such as informing other vendors of vulnerabilities that might impact those and if they alert consumers about fixed vulnerabilities.

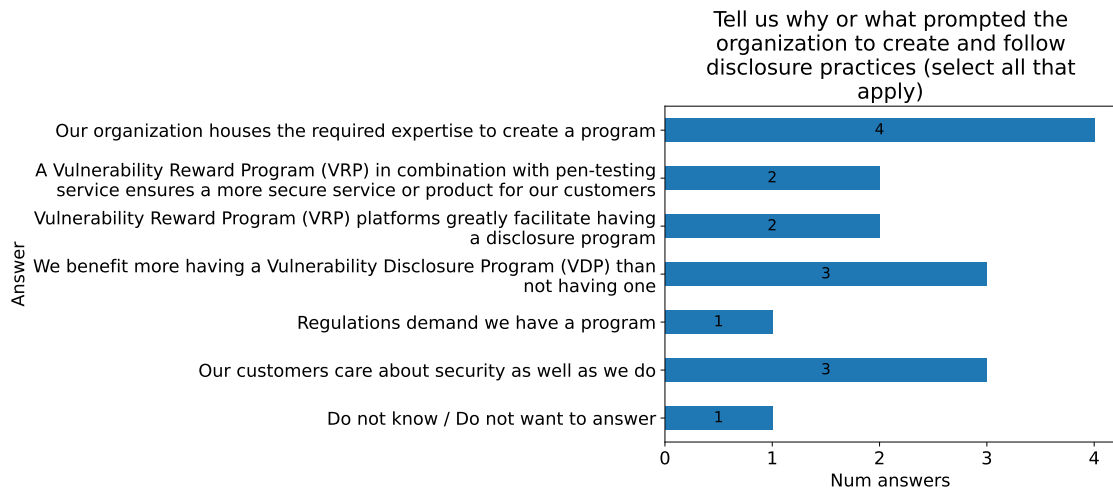
5. Results

Additional questions and answers from those having a VRP

Those participants who answered that their organization had a VRP were asked two additional questions about their VRP practices, as can be seen in Figure 5.1. Figure 5.1a depicts the results from the multiple choice question on what kind of vulnerability disclosure practices participants say that their companies have. The most commonly (four (80%) answers) selected answer option was: “We alert our consumers about fixed vulnerabilities as well as whether we do not fix (discontinued or unsupported products)”. Other common practices with three (60%) answers each were informing and coordinating with other vendors that may be impacted by vulnerabilities reported to them and to have a contact email for reporting vulnerabilities.



(a) Study one: What Practices Do Organizations Have



(b) Study one: What Prompted Org To Follow Practices

Figure 5.1: Study one: Questions for participants that had a VRP

In Figure 5.1b, the results from another multiple choice question are shown: “Tell us why or what prompted the organization to create and follow disclosure practices”. The most common option with four (80%) answers was that their organization houses the required expertise to create a program. Two other popular options with three (60%) answers each were: the companies benefiting more from having aVRP over not having one and their customers caring about cybersecurity as well as themselves.

Additional questions and answer from those not having a VRP

Those 16 participants who answered as not having a VRP were asked seven additional questions to find out more about the reasons why they do not have one. Five out of the seven additional questions were answered by all 16 participants. An aggregated summary of whether it was considered (but then rejected) to create a VRP and whether there is interest to implement one in the future is shown in Table 5.1.

When asked if the company considered creating and implementing a VRP, six (38%) participants said they did not want to or did not know how to answer. Out of the other ten, four (25%) said that their company had considered creating and implementing a VRP and six (38%) said that their organization had not considered it.

In the responses to being asked if their company would be interested in implementing a VRP, nine (56%) participants said that their organization would maybe be interested in implementing a VRP. Only two (13%) participants answered with a “yes” and one (6%) participants answered “no”. Four (25%) did not know or did not want to answer.

When answering if they had a timeline for implementing a VRP, 11 (69%) participants said they did not have a timeline implementing a VRP. One (6%) participant

Question	Yes	No	Maybe	Do not know / do not want to answer
Has the company considered creating and implementing a VRP?	4	6		6
Would the company be interested in implementing a VRP?	2	1	9	4
Do you have a timeline for implementing a VRP?	1	11		4

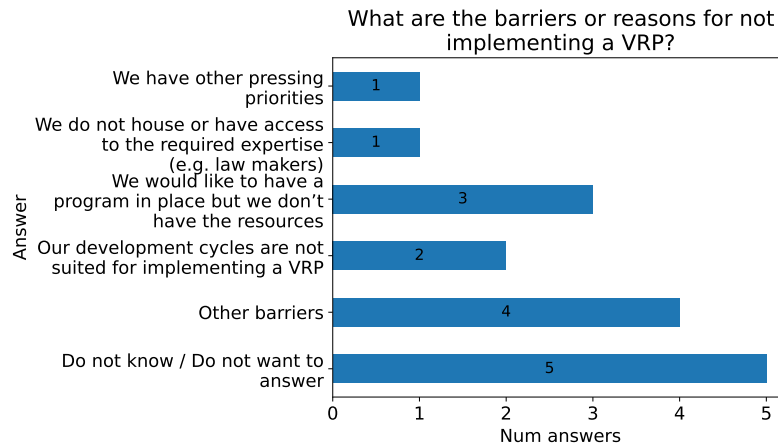
Table 5.1: Study one: Aggregated results from questions around interest in VRPs.

5. Results

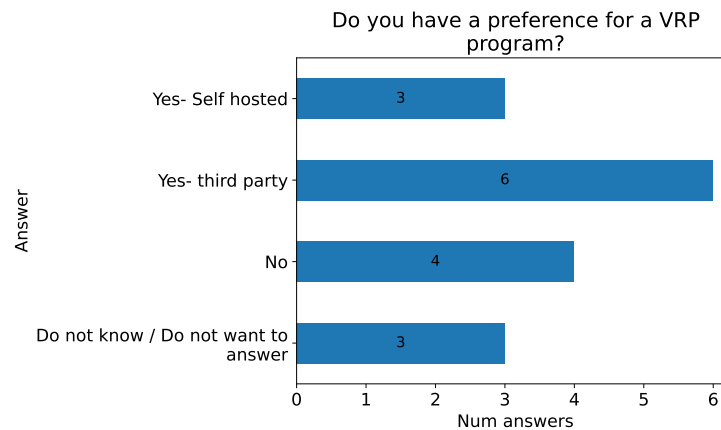
had a timeline for implementing a VRP and four (25%) said that they did not know or did not want to answer.

As can be seen in Figure 5.2a, a lack of resources were the most common barrier from the list of barriers with three (19%) answers. After that, two (13%) participants answered that their development cycles were not suited for the implementation of a VRP. Four (25%) participants chose to answer the question with the “Other barriers” input fields. In that input field, one participant answered that their company was in fact already working on implementing a VRP, one pointed out a need for a dedicated environment as a barrier and two answered that likely nobody had thought about it or that they had never heard about a VRP.

Nine (56%) participants had a preference for a VRP program as can be seen in Figure 5.2b. Of those who had a preference, six (38%) had a preference for third



(a) Barriers to implement VRP



(b) Preference for a VRP program

Figure 5.2: Study one: Questions for those that answered as not having a VRP.

party programs and three (19%) had a preference for a self-hosted program.

A further question was: If your company does not identify benefits of implementing a VRP, why is that? 12 (92%) participants did not know or did not want to answer. Only one (8%) person answered with the free text input field provided for the answer option “other” and the answer was that there is a lack of knowledge.

Awareness

Further questions about awareness of VRPs were asked independent of whether the participant answered whether they have a VRP or not.

As can be seen in Figure 5.3, 15 (68%) participants said that their organization is aware of vulnerability disclosure practices and 14 (64%) thought that their organizations have done something about those practices. Fourteen (64%) participants

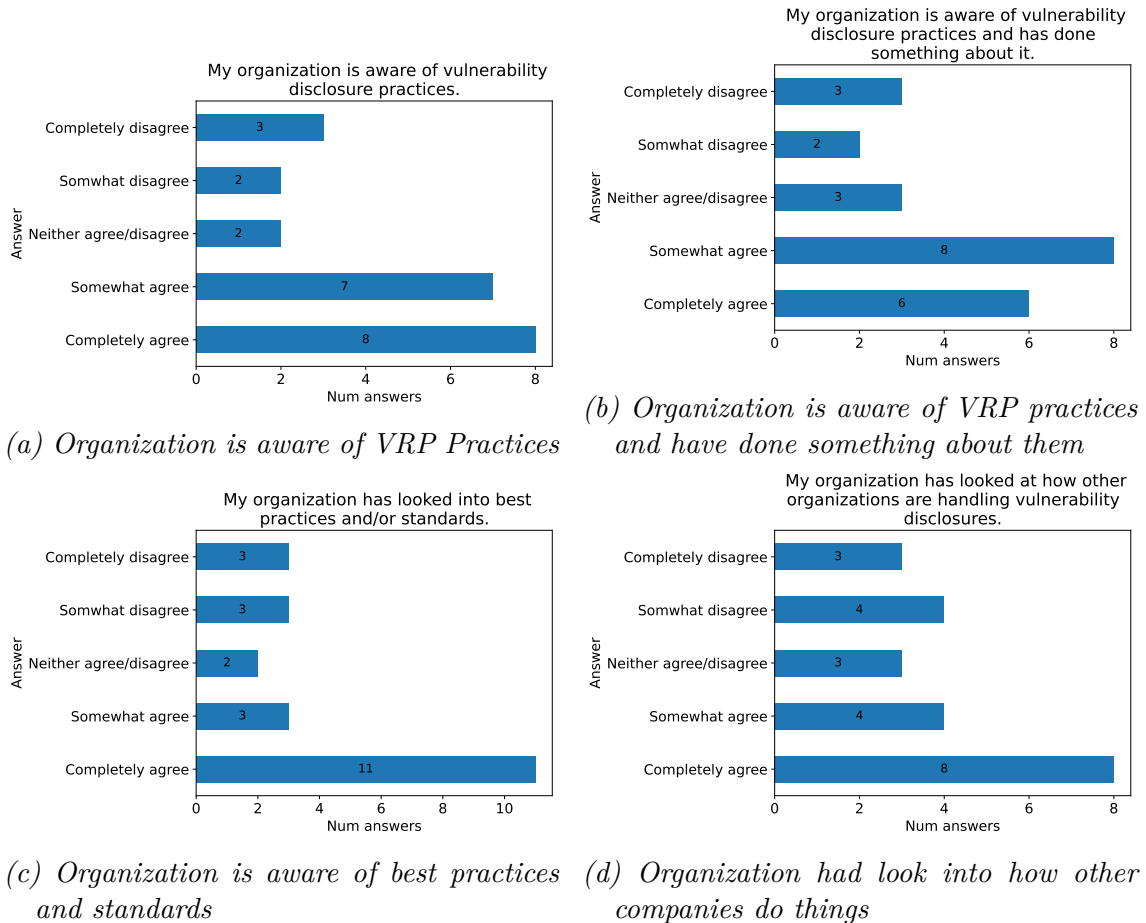


Figure 5.3: Study one: Awareness around VRPs

5. Results

think that their organizations have looked into best practices and standards and 12 (55%) think that their company has looked at how other organizations are handling vulnerability disclosures.

Figure 5.4 shows that a slight majority of participants (55%) rather think that penetration testing is more beneficial than a VRP but also (as well 55%) that VRPs is nevertheless beneficial for their companies. Most (70%) participants think that a VRP would not negatively expose their company but some (37%) think that a VRP program would be too demanding on the company.

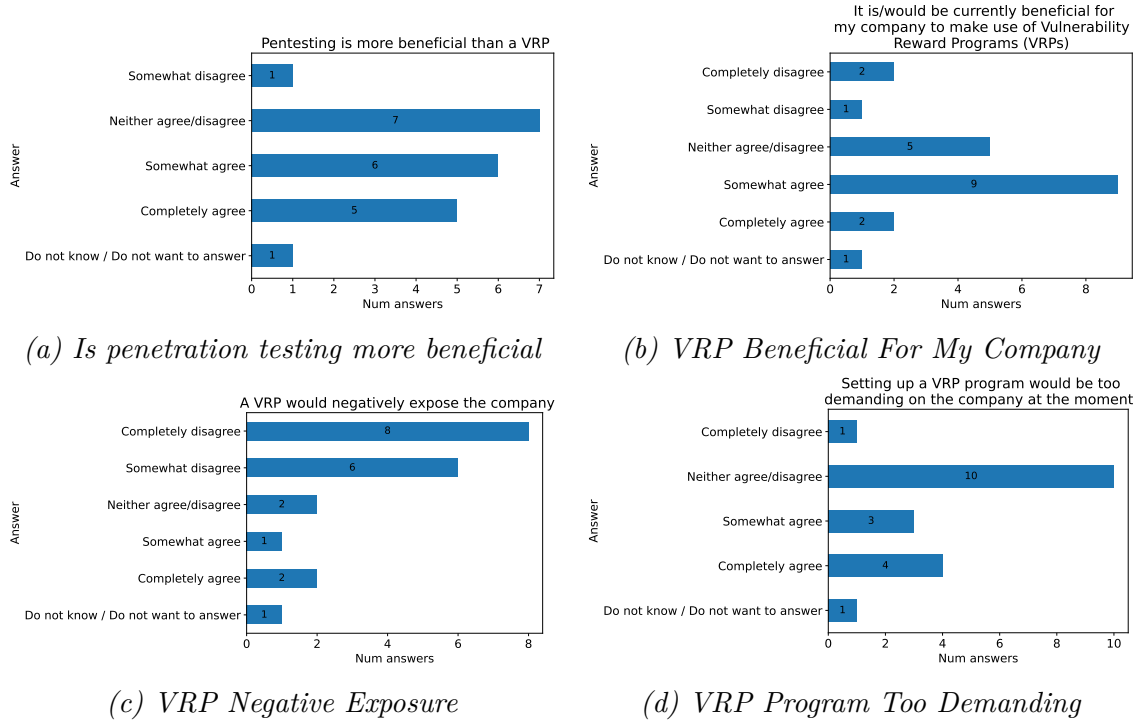


Figure 5.4: Study one: VRP beneficial

Figure 5.5 shows what the participants answered concerning if they were aware of any of the three popular VRP platforms listed (HackerOne, BugCrowd and Intigriti). Ten (45%) participants were aware of one or more VRP programs, though eight (36%) participants were not aware of any of the programs listed and four (18%) answered as not knowing or not wanting to answer.

As can be seen in Figure 5.6, ten (50%) participants do not want any special recognition for their organizations for having a VRP or would like to be anonymous. There are eight (40%) participants in total who want recognition against ten (50%) participants who do not want recognition. Four (20%) of those eight answered that the best recognition would be being on a list of participating companies on the page

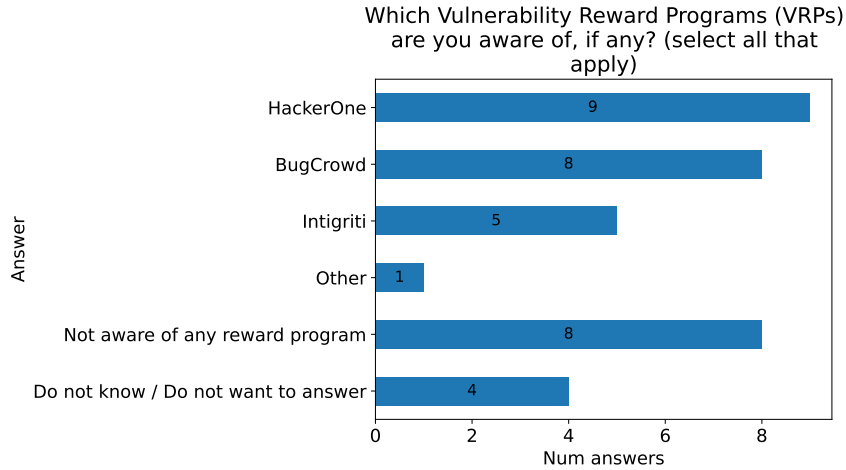


Figure 5.5: Study one: Awareness Of Programs

of the VRP program and four (20%) answered with getting a badge for participating in it.

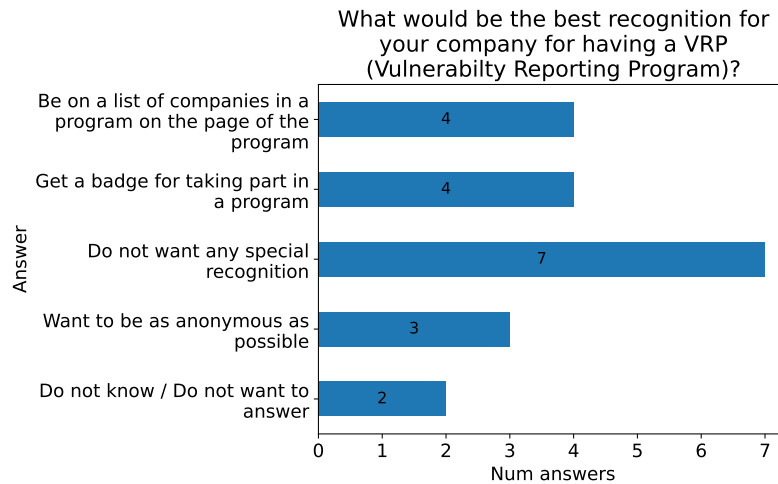


Figure 5.6: Study one: Best recognition for company with VRP

5.1.2. Vulnerability reporting terms suggestions

Because there are no established Icelandic terms for VRP and related concepts, participants were also asked for suggestions for three different VRP terms. As can be seen in Table 5.2, depending on the term, four to six of the participants gave suggestions for Icelandic terms to use in VRPs. Thirteen to 15 participants answered as not knowing or not wanting to answer. The terms that were asked about were

5. Results

terms for VRPs, for a person who looks for and reports vulnerabilities, and for the activity of searching for vulnerabilities.

Vulnerability reporting program	Person who looks for and reports vulnerabilities	Search for vulnerabilities
Villuveiðar	Villuveiðari	Villuveiðar
Veikleika Tilkynninga Gátt VTG	Veikleikaleitari	Veikleikaleitarakerfi
Veikleika vaktarinn	Veikleika veiðir	Upplýsingaöflun
Veikleikaskimun	Veikleika veiðari	Veikleika Veiðiferð
	Veikleikaskimari	Veikleikaskimun
	Upplýsandi	

Table 5.2: Study one: Suggestions from participants on VRP terms.

5.1.3. Cybersecurity, scanning and disclosures

When asked if their organization had a dedicated information security team, 20 (74%) participants said that their organization had an internal security team of one or more people. Only one (4%) participant said that their organization had an external security team and 5 (19%) said that they did not have a dedicated security team.

In Table 5.3, questions with simple yes and no answers are summarized together. Twenty (80%) participants said that their company have application security assessments. Twenty one (78%) participants said that their organization is scanned on a regular basis but only just 14 (52%) of them said that their organization is regularly penetration tested.

When asked, 15 (58%) participants answered that their organization required that staff are trained in software security. There were only eight (31%) participants who answered that their organization did not require it.

In Figure 5.7, 13 (62%) participants said that their organization had received disclosures in the last three years. The most common way of receiving disclosures, with 12 (57%) responses, were through a penetration testing service, next after that with six responses (29%) were disclosures from independent white hat researchers with authorization from the company.

Question	Yes	No	Do not know / do not want to answer
Does your company have application security assessments?	20	5	0
Is your company scanned for vulnerabilities on a regular basis?	21	4	2
Is your company penetration tested on a regular basis?	14	12	1
Does your company require that IT Staff are trained in software security?	15	8	3
Do you have a timeline for implementing a VRP?	1	11	4

Table 5.3: Study one: Results from questions on application security assessments, scanning and more.

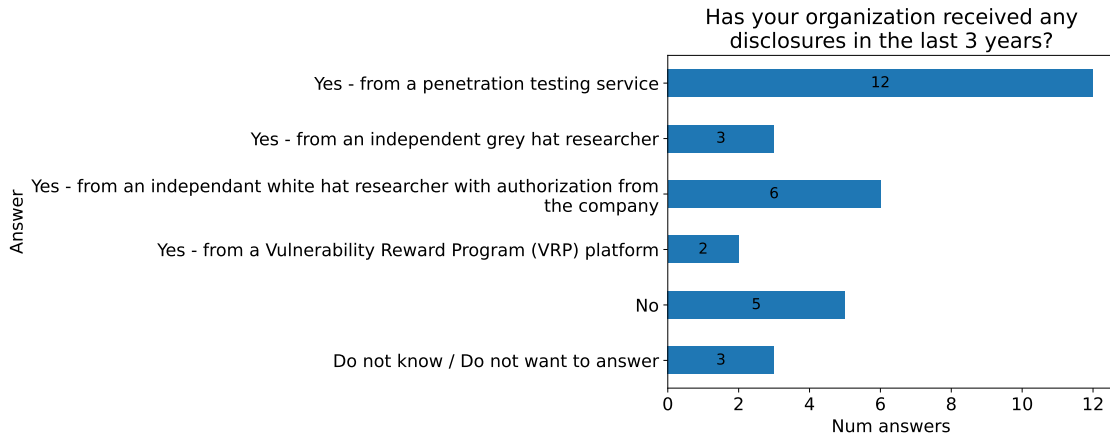


Figure 5.7: Study one: Has Received Disclosures

Those 13 participants that answered “Yes” on having received disclosures in the last three years were asked three further questions about these disclosures.

(Surprisingly, 14 participants answered one or more of the further questions – that is one more than those who answered “yes” to having received disclosures: While that should in theory not be possible, a possible explanation for that would be how SoSci Survey deals with branching: this could happen if a participant first answered “Yes” to having received a disclosure, then answered the extra questions, but then later went back and changed the first answer to a “No”.)

In response to being asked if the organization had pursued vulnerabilities through legal channels, three (21%) participants answered with a yes. Eight (57%) partici-

5. Results

pants answered with a no and 3 (21%) answered as not knowing or not wanting to answer.

When asked if the company had in general been satisfied with the quality of the reports submitted, ten (71%) participants answered with a yes. Two (14%) participants answered with a no and two (14%) with “do not know or do not want to answer”.

The question “Did the disclosure lead to a fix?” was answered with “yes” by all 13 participants who answered that question.

Most participants who reached the last page of the questionnaire did not want to participate in a follow-up interview, in fact only four (20%) of those that reached the last page of the questionnaire said they wanted to do so and left their email address for getting contacted.

5.2. Data from Study two

In this section, the data from Study two is provided. As already described in section 4.1.3, Study two consisted of a questionnaire of a smaller size than in Study one and therefore took less time to take. The participants in Study two were individuals with different backgrounds but the biggest part of those being programmers. This group will be summarized as IT professionals.

The questionnaire in Study two was less detailed than in Study one. It focused on scoping the knowledge of this group of IT professionals on vulnerability reporting and VRPs while still keeping the questionnaire comparable to the main questions in the questionnaire in Study one.

The number of total participants was 71 and after filtering, the total number of data points remaining was 59. The filtering applied was to exclude those that only reached the first page of questions, which contained only demography questions.

Because the questions in this questionnaire are mainly a subset of the questions already asked in Study one, most of the questions discussed in the following are already known from section 5.1. The answers are though of course different as the participants were different.

5.2.1. Vulnerability reporting programs

In Figure 5.8 it can be seen that 18 (43%) participants did not have a preference for whether a VRP program is self-hosted or hosted by a third party. Those who had a preference, rather had a preference for a third party VRP program than a self-hosted VRP program (nine (21%) against 5 (12%) answers). Ten (24%) participants did not know or did not want to answer.

As can be seen in Figure 5.9, when asked about the best recognition for their organization for having a VRP, 14 (37%) of the participants answered as not knowing or not wanting to answer. The other 24 participants answered somewhat evenly. It can though be noted that 13 (34%) of those 24 thought no special recognition or being anonymous was best while 11 (29%) participants opted for some sort of recognition.

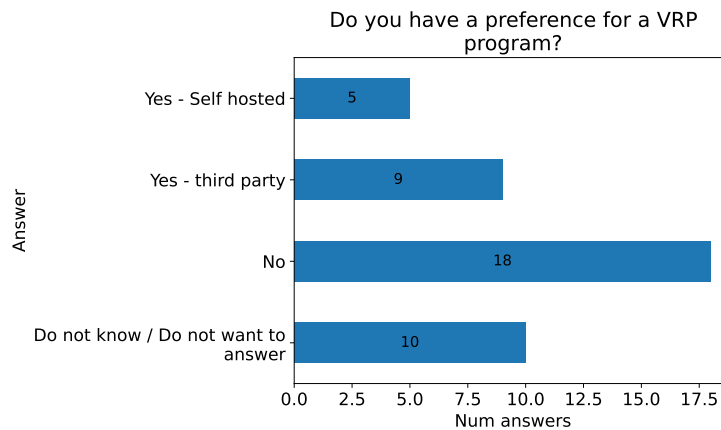


Figure 5.8: Study two: VRP program preference



Figure 5.9: Study two: Best recognition for organizations with a VRP

5. Results

As shown in Figure 5.10, participants were asked if it would be beneficial for their organization to make use of VRPs. From 42 participants who answered the question, 25 (60%) participants either answered as not wanting to answer or not knowing, or answered as neither agreeing nor disagreeing. Of those 17 participants who took a stand on agreeing or disagreeing to VRP programs being beneficial, 13 (31%) agreed and only four (10%) disagreed.

In the question, “If you/your organization does not identify benefits of implementing a VRP, why is that?”, 22 (59%) participants answered that they did not know or did not want to answer as can be seen in Figure 5.11. From those that did answer, ten

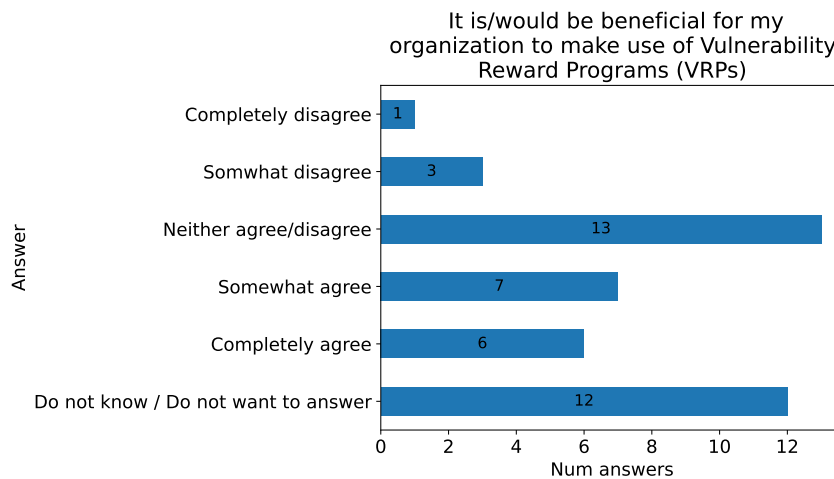


Figure 5.10: Study two: The beneficiality of making use of VRPs.

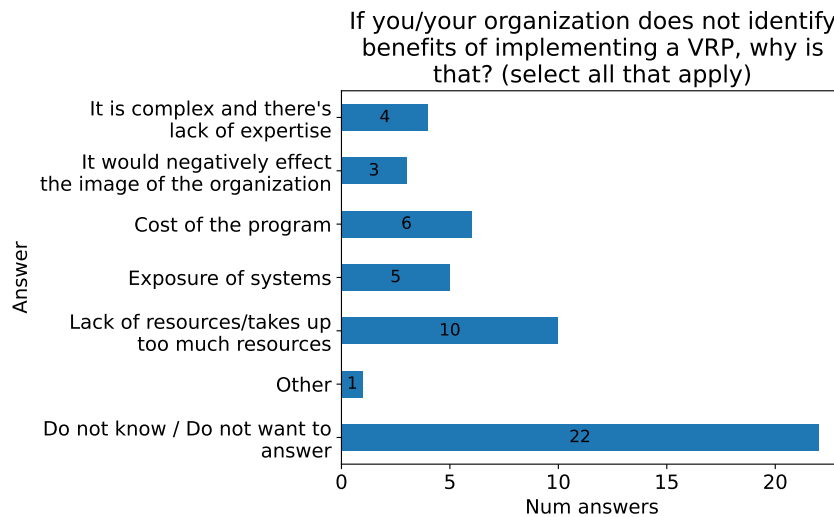


Figure 5.11: Study two: Why do organizations not identify benefits of implementing a VRP?

(27%) said there was a lack of resources and six (16%) answered as the cost of the program being a reason of organizations not identifying benefits of implementing a VRP.

In Figure 5.12, 22 (52%) participants answered that they were not aware of any reward program platform. The platform that was best known was HackerOne with seven (17%) answers. In total, 11 (26%) participants knew one or more VRP platforms.

In the multiple choice question in Figure 5.13, participants were asked to mark all the items that fit with respect to VRPs for their organization: Thirty one (67%) participants answered as not knowing or not wanting to answer. Of those 16 (35%) that answered other than not wanting to answer, the most popular answer with

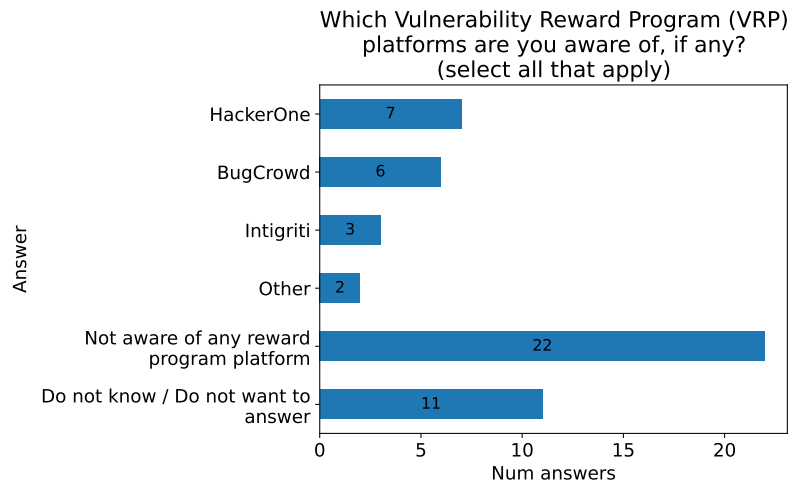


Figure 5.12: Study two: Best known VRP platforms

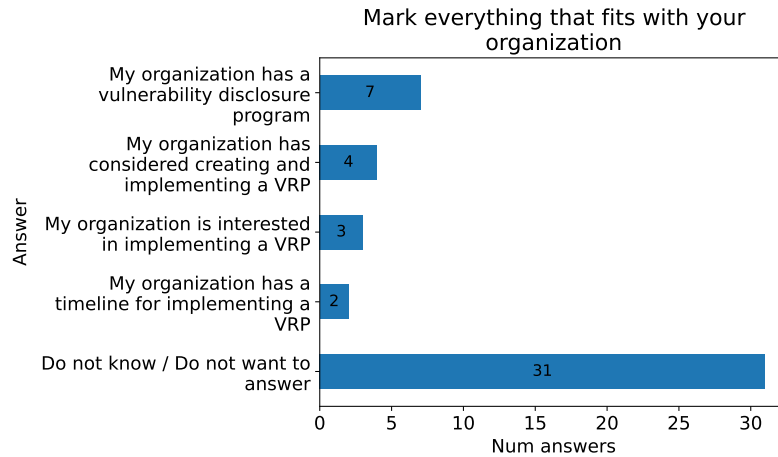


Figure 5.13: Study two: Interest in implementing VRP and other considerations

5. Results

seven (15%) answers was that of the organization having a vulnerability disclosure program.

5.2.2. Security, scanning and disclosures

The question depicted in Figure 5.14 asked if penetration testing was more beneficial than a VRP. There, 29 (71%) participants again either answered as not wanting to answer or not knowing, or answered as neither agreeing nor disagreeing. Of those 12 (29%) participants who took a stand on agreeing or disagreeing to penetration testing being more beneficial than a VRP, ten (24%) agreed and only two (5%) disagreed.

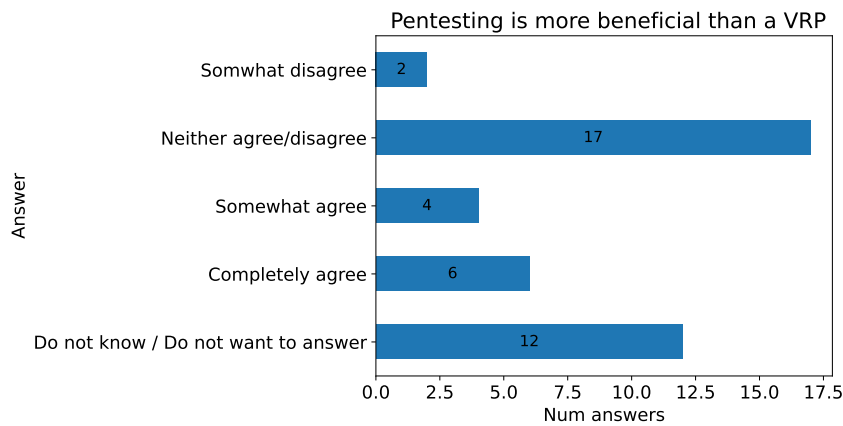


Figure 5.14: Study two: Is penetration testing more beneficial?

Figure 5.15 shows how participants answered with respect to whether their organizations have received disclosures in the last three years and from what source. There were 42 total responses to this multiple choice question and of those, 18 (43%) answered as not knowing or not wanting to answer. Apart from that, 18 (43%) participants selected one or more different options of having received disclosures and only 6 (14%) participants answered that their organization had not received any disclosures.

Those participants who answered that their organization had received disclosures in the last three years were asked additional questions about disclosures, which are aggregated in Table 5.4. From these additional questions, it can be seen that nine (56%) participants thought that their organizations had been satisfied with the quality of the reports submitted and only two (13%) participants said that they were not satisfied with the quality of reports. Fourteen (88%) participants also said that the disclosures led to a fix. Twelve (75%) participants said that their organization

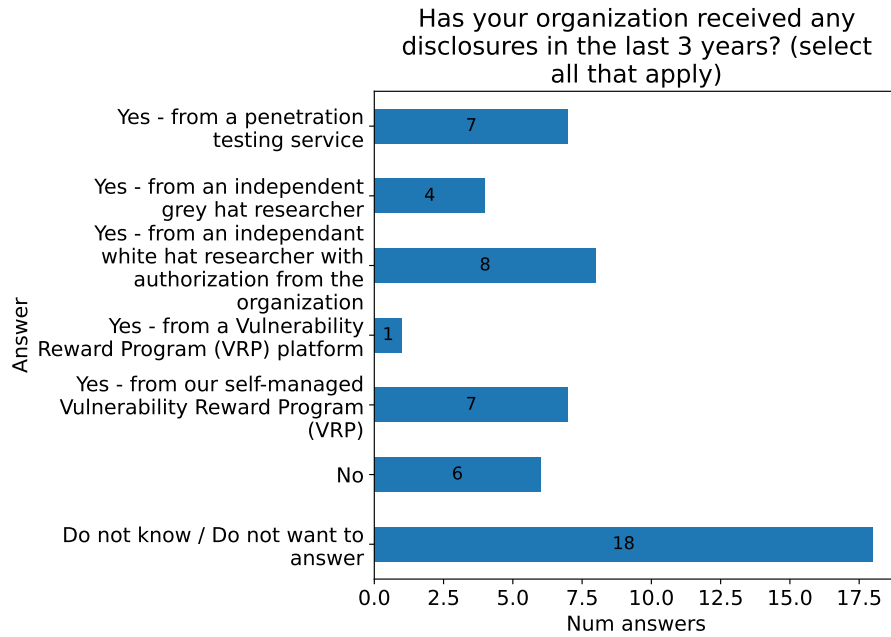


Figure 5.15: Study two: Received disclosures in the last 3 years

had not pursued disclosures through legal channels, the other four (25%) said that their organization had done so.

Question	Yes	No	Do not know / do not want to answer
In general, has your organization been satisfied with the quality of report(s) submitted?	9	2	5
Did the disclosure lead to a fix?	14	1	1
Has the organization pursued vulnerability disclosures through legal channels?	4	12	0

Table 5.4: Study two: Results from questions on received disclosures. The rows show the questions and the columns show the answers, counted in number of answers.

As can be seen in Figure 5.16, 24 (56%) participants said that their organizations require IT staff to be trained in software security. Thirty (70%) participants also said that their organizations have application security assessments and 37 (86%) participants said that they were scanned for vulnerabilities on a regular basis by the request of the company. Only 17 (40%) participants answered that their organization was penetration tested on a regular basis.

5. Results

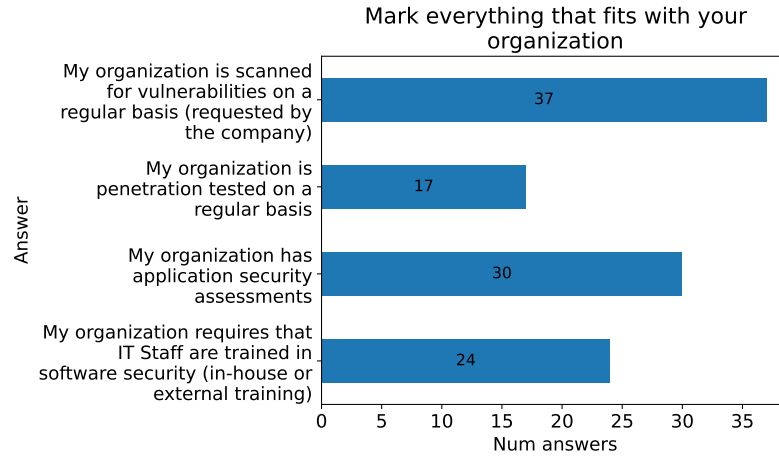
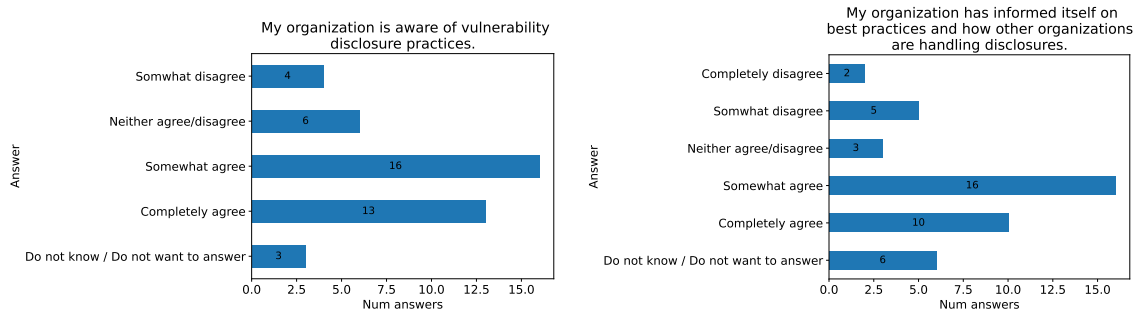


Figure 5.16: Study two: Training, assessments and scanning



(a) Awareness of vulnerability disclosure practices (b) Organizations informed on best practices



(c) Have organizations done something about vulnerability disclosure practices

Figure 5.17: Study two: Questions on awareness and information.

Figure 5.17 covers answers to three different questions. Figure 5.17a shows that 29 (69%) participants think that their organizations are aware of disclosure practices and from Figure 5.17c it can be seen that 28 (67%) participants said that they had done something about them. According to Figure 5.17b 26 (62%) participants also think that their organizations have informed themselves on best practices and how other organizations handle disclosures.

5.3. Data from the interviews

In this section the interviews conducted in Study one are presented by providing summaries in a way that the interviewed individuals and their companies cannot be identified.

5.3.1. Interview one

In Interview one, the interviewee said that their organization had not received any disclosures in the last ten years. Even so, they think that receiving disclosures from ethical hackers is of great value, and they had started looking into if they should set up a VRP. They thought that VRPs are low maintenance, as the simplest form of a VRP is a simple text site on their website. This could as an example be part of the `/security.txt` [8] file on their company's website. This text site would only need to state what the program allows and how to disclose vulnerabilities to them. The organization also knew of two companies with VRPs. They pay security contractors to penetration test their systems, and they have a good security budgets to utilize for that. They are not compliant to specific standards, but they rather have their own standards and try to test the systems in different ways with their budget. They said that they buy time from a security contractor company every month for testing and have at least one big penetration test performed every year.

They did not think that there are many ethical hackers in Iceland currently and that the surrounding culture is not there yet. That could though change if it comes more common in Iceland to have a VRP. They think that one benefit of having a VRP is that it shows the outside world that they care about security. They get a lot of attention and attacks from the bad guys, and they say that bad actors try to simply hack somebody, not necessarily some specific company. Therefore, having a system that looks secure could work to incentivize bad actors from attacking their systems. Having a VRP could also be a factor that has an effect on the insurance.

They have a non-mandatory awareness program for employees for phishing. They tracked how many employees take it, though they want to have an attendance score at some point that they can improve on. They have a code of conduct their personnel need to follow. They have an extensive internal security scanning where they scan every network every week along with scanning their network from the outside every month. They try to automatically update as much as they can. They try to keep track with vulnerabilities in their products, for example by email lists from vendors or from the Icelandic CERT. If they got a disclosure, the person would get good recognition, especially if they would apply for a job with them later on.

5. Results

The company would never go after a disclosure legally, and if that would happen the interviewee would not stay with the company. They think that the company should take part in a free VRP in Iceland, even though they probably would not get any disclosures. When the interviewer mentioned the possibility of creating a nation-wide VRP in which all companies would be part of, following an opt-out model, they said that they thought that it would be better to take part in it to make it likelier that other organizations take part as well. They felt that an opt-in implementation VRP would be better if a national VRP was created as otherwise companies might get angry and give cybersecurity researchers the wrong idea of it being fine to hack companies that are not fine with it. They thought that this kind of platform would be very interesting and mentioned that there are individuals that hack just for fun or recognition.

5.3.2. Interview two

In interview two, the interviewee thought that their organization had improved their vulnerability disclosure practices a lot. They furthermore had a positive outlook on BBP, and they had worked at an organization with a BBP before. In fact, that organization eventually stopped scanning their systems as they found that they were being sufficiently scanned by security researchers in the BBP. They think that for a VRP to work, there needs to be a bounty. From their experience with BBPs, they mentioned that there are a lot of false positives reported and to properly respond to disclosures, resources are needed.

Their organization had looked into BBP but the sensitive nature of the data in their systems proved to be a barrier to implementing one, even as a private BBP, data would need to be used for the system to be functional. For an organization with sensitive data, artificial data would need to be created along with a testing environment to run the program on, which involves time and proper resources to get done. Their organization therefore did not have a VRP even though there was interest for having one. That was though not the only reason for not having a BBP, as they also mentioned that they already have enough to work on trying to address vulnerabilities that they already know of. Many individuals playing with a system with information of sensitive nature could also have adverse affects.

They have an internal program that lets employees report vulnerabilities, which could be called an internal VRP. They have gone from scanning one or two times a year to regular scanning and are penetration tested on a regular basis. Their view on penetration testing is that it is inexpensive and should be used. They do internal security training through seminars, training material and training tests. They also keep up with reported vulnerabilities from products and systems they use. When the interviewers mentioned a badge-style recognition for companies with VRP, they

said that they did not want any badge as recognition for their organization if they took part of a VRP. They also did not think the cyberattacks had increased at the time of taking the interview.

5.3.3. Interview three

In interview three, the interviewee said that they did not have a disclosure policy, but they are ISO 27001 ¹ certified. Therefore, they have security policies in place for how they deal with vulnerabilities that are publicly disclosed. They want disclosures even though they do not have a VRP. They thought about having a `security.txt`, and they started adding it to their system, but did not finish doing so. They think that not many companies have a `security.txt` [8].

They are not interested in implementing a VRP because they generally do not have any code, they write it for their customers, it is the customers code. They only have a WordPress site publicly available on their system. They have though been indirectly part of the chain of a disclosure, they have written software for a customer that was part of the chain of software that became affected because of a vulnerability. They had a discussion already on the topic of taking legal action against researchers. They said that they would be happy to get disclosures and would not go after anyone, they see it as somebody doing them a favor. They think that having a green checkmark that says that companies are part of VRPs would just be a money making scheme, and that it would be better to have a shame list.

If there would be a nationwide BBP then they think it would be different, good to have a directory of companies with a BBP. Their company is regularly scanned but is not penetration tested regularly. One service they provide is actually to scan systems of customers. For example around Docker files. They do proper scanning but no penetration testing.

Most of the employees have a lot of experience, and they would not go to security training. They keep themselves up to date and go to security seminars even though they do not have any official training. They do patching of vulnerabilities in database systems and along with scanning that is relevant to their customers. They know what is important and what is not important around patching database systems.

When asked about Icelandic terms for the English term hacker, the interviewee did not have a negative connection to the Icelandic term for hacker, *hakkari*. They did though mention that in the media it is a negative term. They would rather like to have penetration tests with full access to the code on site instead of a bug bounty.

¹The ISO 27001 is a information security management systems standard, and being ISO certified means that the company has to have a system to manage security risks regarding data that the company owns or is handled by the company.

5. Results

They would rather make a copy of the production system to for testing, and would like to have trusted individuals to penetration test their system. Furthermore, they thought that capable security professionals that know what they are doing are more valuable. The said that the companies that have BBP in place are the big software vendors that can test everything.

6. Discussion

The previous chapter presented the study data as aggregated results. These results will now be discussed in this chapter and conclusions are drawn from these.

6.1. Discussion and conclusions

In Study one, individuals in managerial positions were asked about their views on VRPs in relation to their organizations. In Study two, individuals with a more general background in programming were also asked about VRPs in relation to their organizations. The questions used in the questionnaires of these two studies were for a big part the same questions, and therefore also a comparison can be made between the different groups that answered these questionnaires.

When the participants were asked if their organization had a vulnerability disclosure program, most answered as them not having one. In Study one, 27% answered having a VRP and 62% of participants answered having no VRP. In Study two, only 15% answered as having a VRP when asked to mark all items that fit to their organization in a multiple choice question and 67% answered “Do not know/Do not want to answer”. The question with all its options can be seen in the Appendix, chapter A.

That difference is likely caused by better knowledge of their organization by the management-centric participants from Study one in comparison to the broader group of IT professionals from Study two. Furthermore, Study one is more biased towards cybersecurity awareness and therefore, the covered companies are more likely to have a VRP.

It can also be seen from the 2022 HackerOne report [11] that 42% of those hackers who have skipped reporting a vulnerability they had discovered said that the reason was the lack of a disclosure program.

Conclusion 1 The usage of VRPs is low in Iceland.

6. Discussion

This means, there is a lack of disclosure channels through which a vulnerability can be disclosed and that hackers that take part in VRPs do not necessarily disclose vulnerabilities if there is no disclosure program. By adding a simple VRP, organizations could make disclosing vulnerabilities more straight forward and easier.

Conclusion 2 In comparison to the general IT professionals from Study two, the managers in Study one seem to have more knowledge of what their organizations are doing in regard to cybersecurity.

Obviously, the demography of the targeted groups matters. In further studies, depending on what kind of information is being sought, it would be better to ask managers and cybersecurity professionals about the more detailed aspects of cybersecurity in their organization. This way, the quality of data will be higher as lack of participants knowledge may skew the results through them answering about things that they do not know much about. It would be good to ask general IT professionals questions that are less specific and more about the security culture of the organization.

On the other hand, getting IT professionals to participate also proved easier than getting managers to participate in the studies.

6.1.1. Disclosures and Penetration testing

Participants in both studies were asked if their organizations had received disclosures in the last three years. Sixty two percent of participants in Study one said they had received disclosures versus 43% in Study two.

In Study one, the most common response with 57% of answers was having received disclosures from penetration services, followed by 29% mentioning disclosures received from independent white hat hackers with authorization from the organization. In Study two, the most common answers were disclosures from independent white hat hackers with authorization from the organization with 19% of answers, disclosures from a penetration testing service with 17% of answers and disclosures from their self-managed VRP with 17% of answers.

In Study two, 43% of participants versus 14% of participants in Study one answered as not knowing or not wanting to answer. This difference between the studies in number of participants answering as not knowing or not wanting to answer confirms Conclusion 2.

Twenty four percent of participants answered as not having received any disclosures

in the last years in Study one and 14% in Study two.

Conclusion 3 The most common means of receiving a disclosures in the questionnaires were penetration testing and other cybersecurity researchers with authorization.

This might be because of the lack of vulnerability reporting channels in organizations. If cybersecurity researchers already have authorization, they should already be in contact with the organization and know what they can do and who to inform on any vulnerability findings. This means that the lack of a public channel through which to report a vulnerability to the organization does for the most part not affect them. This is not the case with unauthorized cybersecurity researchers, who have this barrier to report a found vulnerability, they need to look for a way to report it and take a risk in not knowing if the organization will respond positively to the vulnerability disclosure.

Nevertheless, there was though a good number of disclosures from cybersecurity researchers without authorization, and it would be reasonable to expect that this number would increase even more if this barrier would be removed by having a public disclosure channel.

In addition, the participants were asked if their organization had been satisfied with the quality of the vulnerability reports submitted. In both studies, most participants said that their organization had been satisfied with the quality. In Study one, 71% of participants answered “yes” and in Study two 60% of participants answered “yes”. So, for this question the results were similar in affirming that most participants thought the report quality was good.

Conclusion 4 Most of those participants who had received disclosures were happy with the quality of vulnerability reports.

That points to the quality of reports not being a common problem in vulnerability reporting, so putting an increased focus on report quality in a VRP would likely not pay off for most organizations.

6.1.2. Quality of disclosure reports and vulnerability disclosures that led to a fix

When those participants who received disclosures were asked if the disclosures lead to a fix, most all answered positively. In Study one, all 13 participants answered with “yes” and in Study two, at least 88% answered with “yes”.

Conclusion 5 In general, organization that receive disclosures, fix the reported vulnerabilities.

However, it is not known if that would change with an increased number of disclosures as the number of disclosures may not have been large so far. If organizations take part in a bug bounty, there could for example be a large influx of disclosures of vulnerability reports which the organization would need to be prepared to take care of.

Because of disclosures currently leading to a fix, that threshold where organizations do not have the capacity to take care of all disclosures does not seem to have been reached, yet. Increasing the number of reports closer to the organization's limit in capacity in processing vulnerability disclosures should therefore still be possible to a certain extent without the organizations to be overwhelmed with the number of disclosures.

6.1.3. Legal pursuit of vulnerability disclosures

In both studies, the proportion of participants who said that their organization had pursued vulnerabilities legally was quite even. Twenty one percent of participants in Study one answered with “yes” while 25% answered “yes” in Study two.

As already described in Section 2.1.4 of Chapter 2, the 2022 HackerOne report [11] states that 12% of those hackers who have skipped reporting a vulnerability they had discovered (50% of hackers on the platform in both 2021 and 2022) said that the reason being threatening legal language.

This fear of hackers of legal implications seems to be valid in Iceland: over 20% of respondents in both studies answered that their organizations had pursued vulnerability reporters legally.

Conclusion 6 If theses fears of legal implications of reporting vulnerabilities were reduced, there would be a likelihood of an increase in the numbers of disclosures in Iceland.

6.1.4. Type of VRP

Fewer participants in Study two had a preference for a particular type of VRP program (self-hosted vs. third party). That is, 56% in Study one and 33% in Study two. This may again be a confirmation of Conclusion 2.

In both studies, there was a similarly high ratio of respondents who said that they had a preference for third party VRPs over self-hosted ones: in Study one, the ratio was six against three (2:1) and in Study two the ratio was nine against five (1.8:1).

Conclusion 7 More participants have a preference for a third party VRP than a self-hosted one.

6.1.5. Best recognition for organization

The results from the question on the best recognition for the participant's organizations for having a VRP are somewhat similar in both studies. The main difference is that much more (10% in Study one versus 37% in Study two) participants answered as not knowing or not wanting to answer in the Study two (confirming again Conclusion 2). Another difference is that more participants in Study one (50% versus 34% in Study two) answered as not wanting any special recognition or being anonymous in the first study.

If the options are grouped together as “want to have recognition” and “do not want recognition” or to be anonymous, the answers are almost even between the two studies. In Study one, 50% of participants answered as wanting no special recognition and 40% of participants answered as wanting recognition. In Study two, 34% of participants answered as not wanting recognition and 29% of participants wanted recognition.

Conclusion 8 A number of participants do not want recognition for taking part in a VRP.

Therefore, it would be good to have an opt-in list of participants on the site of the program if one is created. That way, those who want recognition can have it by opting in and those who want to be more anonymous can remain so.

6.1.6. Awareness and being informed

The participants in both studies mostly agree that their organization is aware of disclosure practices, the organization has informed itself on them and has done something about them (see figures 5.3 and 5.17 in Chapter 5).

For their organization being aware of vulnerability disclosure practices, 68% of participants said in Study one said so and in Study two 69% said so. In Study one,

6. Discussion

64% of participants said that their organizations have done something about those practices and 67% said so in Study two. Sixty four percent of participants in Study one think that their organizations have looked into best practices and standards and 55% think their organizations have looked at how other organizations are handling vulnerability disclosures. In Study two, 62% of participants think that their organizations have informed themselves on best practices and how other organizations handle disclosures.

Conclusion 9 Organizations claim to have knowledge about disclosures and how to handle them, even though not many have thought about creating a VRP. This base of knowledge is a good foundation for creating VRPs.

6.1.7. Is it beneficial to make use of VRPs and Penetration testing

The responses in both studies had a similar outcome on the beneficiality of VRPs: most participants thought about VRPs as being beneficial for their organization. In Study one, 55% of participants thought VRPs would be beneficial and in Study two the ratio was

Conclusion 10 Many participants think that VRPs are beneficial, but implementation is low along with awareness. The awareness needs to be increased, for example through the creation of a national VRP.

31%. In Study two, 60% of participants either answered as not wanting to answer or not knowing, or answered as neither agreeing nor disagreeing. In Study one, that ratio was 35%, thus confirming again Conclusion 2.

When participants were asked if penetration testing was more beneficial than a VRP, those participants who took a stand generally said that was true. In Study one, 55% thought so while only 24% thought so in Study two. This huge difference can be explained by more unsure answers in Study two, 71% of participants either answered as not wanting to answer or not knowing, or answered as neither agreeing nor disagreeing, meanwhile the ratio in Study one was only 40%.

6.1.8. Why do some organizations not identify benefits of implementing a VRP

When participants in Study one were asked about the reason for their organizations not identifying benefits of implementing a VRP, all but one participant (92%) did not know or did not want to answer. In Study two, fewer participants (59%) answered as not knowing or not wanting to answer. Therefore, a hypothesis can only be made by looking at the few who did provide reasons in their answers: in Study two, twenty seven percent said that there was a lack of resources and 16% answered as the cost of the program being a reason.

Conclusion 11 Costs and lack of resources might be a reason for not having a VRP.

To get organizations to adopt VRPs in bigger numbers, having a VRP can be made easier and cheaper by for example creating a national VRP in Iceland that is free for organizations to take part in and help them with the effort of validation of vulnerabilities reported through that VRP. This is though only a hypothesis as most participants did not want to answer.

6.1.9. Best known VRP platforms

Participants were asked what VRP platforms they were aware of, if any. They could select from three listed popular VRP platforms or specify other platforms. In Study one, more participants (45%) knew of platforms than not (36%). Eighteen percent answered as not knowing or not wanting to answer. In Study two, more participants (52%) answered as not knowing any VRP platforms than answered (26%) as knowing platforms.

Conclusion 12 VRP platforms are better known in management.

6.1.10. Training, assessments and scanning

In both studies, a similar ratio of participants said that their organization requires that IT staff are trained in software security. In Study one 58% said so and 56% said so in Study two. More participants in Study one (81%) said that their organization has application security assessments in comparison to Study two (70%). In both studies, most participants (78% in Study one and 86% in Study two) answered as the company being scanned for vulnerabilities on a regular basis (requested by the company). Meanwhile, in Study one, the number of participants who said that they

6. Discussion

were penetration tested on a regular basis was around half (52%) and in Study two 40 % of participants answered affirmatively.

That is a relatively high percentage when compared to 31.7% of 1100 participants from 59 different countries answering that external penetration testers were used to identify security problems, as was mentioned in chapter 3. The results from the questionnaire were though only provided as an average over all the countries, not by individual country, so they can not be used for comparison of the use of penetration testing in Iceland and neighboring countries [21].

Conclusion 13 Around half of organizations are penetration tested on a regular basis.

The relatively high percentage of participants saying that their organization is penetration tested is surprising but positive, as for the securing of a software system, penetration testing is of the utmost importance.

The ratio of participants who reported that their organizations were scanned on a regular basis was though considerably higher. In Study one, 78% said their organizations were scanned on a regular basis and in Study two the percentage was 86%.

Conclusion 14 Most organizations are scanned on a regular basis.

Even though the ease of reporting from having a VRP and the use of BBPs have a good effect on the cybersecurity of an information system, not many companies have VRPs. In both studies, almost no participants answered that their organization had a timeline for implementing a VRP (6% in Study one and 4% in Study two). In Study two there were only 7% of participants who answered as their organization having interest in implementing a VRP, the results in Study one were similar but in that study, the participants were given the option of answering with “maybe” and many (56%) answered as their organization maybe having interest but only 13% of participants answered with a “yes”. In Study two, almost no participant (9%) answered that their organization had considered creating and implementing a VRP but in Study one 25% of participants answered yes. In Study two 15% of participants answered that their organization had a VRP, meanwhile in Study one 25% said so.

Conclusion 15 Not many organizations have considered creating a VRP.

The fact that organizations have not (only 25% answered that they had in Study one) necessarily considered creating and implementing a VRP, points to a lack of interest in VRPs. However, this is not necessarily the case: One other possible reason for why organizations have not considered it is that not

all organization have good knowledge of what VRPs are. As an example, only 45% of participants reported as knowing any VRP platforms in Study one. Other possible reasons for not considering creating a VRP are cost and a lack of resources.

6.2. Most important findings

In this section, the most important findings will be summarized and put into the context of the research questions from Chapter 1, i.e. the state of VRP in Iceland, barriers affecting the use of VRP, and how commonly penetration testing and system scanning are used in Iceland. Also, further findings that cover topics beyond the research questions are discussed.

6.2.1. The state of Vulnerability Reporting in Iceland

The two studies show that most of the participant's organizations know best practices around disclosures and how to handle them. However, not many organizations have though considered creating and implementing a VRP which points at a lack of interest or knowledge on VRPs. Only 45% of participants in Study one knew one or more VRP platforms which points at a lack of knowledge of VRP even though they may have knowledge on vulnerability reporting in general.

6.2.2. Barriers that affect the use of VRPs

Barriers with respect to VRPs were found for cybersecurity researchers who want to report vulnerabilities and as well for organizations offering VRPs. One of those barriers is that there is a lack of a reporting channel for most organizations. A fear of legal implications from reporting is another barrier. These barriers can be solved by having a simple VRP with information about what is the best channel through which to disclose vulnerabilities, what the rules of the program are and assurance that reporters of vulnerability will not be legally persecuted if they follow the rules of the program.

The most common reason for organizations not to implement a VRP was a lack of resources. Low report quality generally was not a problem and the number of reports did not appear to be too high for organizations as most of them are capable of addressing the vulnerabilities reported.

6. Discussion

To help alleviate the resource cost of having a VRP and get more organization to implement one in bigger numbers, the thesis author recommends the creation of a national VRP program that is free for organizations to take part of. It would be advised to have a VRP program that allows cybersecurity experts to send in reports of vulnerabilities for any organization in Iceland and that the program would send the report forward to the organization that owns the software infrastructure that the vulnerability report refers to. This program would preferably be free of charge to organizations, so that it would be less problematic to include all organizations in Iceland in the program, that is that the organizations do not need to pay out a bug bounty to the reporters of the vulnerabilities. This would therefore not be a paid BBP, but a non paid VRP. Furthermore, to help with the cost of organizations of validating the vulnerabilities, it would be recommended that the program would validate each vulnerability report before sending them on to the organizations.

Creating a national VRP for Iceland would likely also increase the number of vulnerability reports in the nation. Some organizations might though like to be as anonymous as possible, so if this kind of program would include a list of organizations that take part of it, the author would advise to have that list opt in so that those organizations that prefer to be anonymous can remain so.

One of the supposed benefits from having a VRP such as a BBP, is though that it is thought as being cheaper than paid penetration testing because of only needing to pay for found vulnerabilities but not for the general work of penetration testing. This is likely correct for systems that are already considerably secure, as not a lot of easy to find vulnerabilities will start flooding in, but rather only harder to find vulnerabilities in a lower number. In less secure systems, there is a possibility of having a flood of disclosures that lead to having to pay out large sums of money. One way to solve that could be to have a cap of total monetary rewards for the program, such that the bug bounty program is only active as long as there is still money left to pay out. That way, the cost of the program will not be unexpected high.

For some organizations, the cost of the program is not the problem, but rather bringing attention to a vulnerable system. This was the case for the participant in Interview two (see section 5.3.2), where there was a will for creating a BBP but because of sensitive data and already having enough work to do with addressing vulnerabilities already, a BBP was not created. For sensitive systems that can not handle attacks well, it is recommended to have an invite-only bug bounty where cybersecurity researchers are allowed to penetration test a copy of the production system that does not affect critical infrastructure or systems but can shed a light on important vulnerabilities in the system.

6.2.3. The use of penetration testing and system scanning used Iceland

It could be seen from the studies that a big majority of organizations are scanned on a regular basis, but only around half of organizations are regularly penetration tested. In Interview two in section 5.3.2, the participant also pointed out that they thought that penetration testing was inexpensive.

6.2.4. Other findings

Participants from the management group (Study one) answered less often as not knowing or not wanting to answer than the IT professionals group (Study two). The managers likely have more knowledge of cybersecurity and vulnerability reporting as well as what their organizations are doing regarding those, for example they knew more VRP platforms than the IT professionals. Therefore, a group formed of management professionals or a group with a similar base of knowledge on cybersecurity and vulnerability reporting would be preferable to a group of IT professionals when asking questions in a questionnaire around those subjects in a relatively challenging way. If the questions revolve around general cybersecurity culture, IT professionals would likely be a better group as they are more numerous and therefore easier to get more participants than in the management group.

6.3. Limitations of this thesis

This section discusses limitations of this thesis that may be considered a threat to its validity.

6.3.1. Small size of data-set

A limitation of this thesis is that because of the small size of data-sets, statistical outliers may have a big influence. This also means that the results are more anecdotal in nature and not necessarily statistically significant.

6.3.2. Selection method of participants may lead to bias

One limitation of the research in this thesis is that the data in Study one is likely optimistic towards cybersecurity awareness. This is because many participants were invited to participate in the questionnaires through the networks of cybersecurity professionals. Study two might on the other hand have had a too broad selection of participants as more participants answered as not knowing or not wanting to answer than in Study one.

6.3.3. Distribution

In the distribution of the questionnaires, additional social media platforms could have been used, like X. The reason that this was not done was that Facebook and LinkedIn are widely used in Iceland and the questionnaire only focused on individuals working in Iceland. It can also be noted that not a huge number of participants were recruited through these platforms, though they did help, but rather the biggest number of participants were recruited through the professional networks of the supervisors of this thesis. Furthermore, cold calls through LinkedIn could have been used. This was not done as the amount of data was deemed sufficient and the time doing this could have put the deadline of submitting this thesis in danger.

6.3.4. Why were not more interviews performed

The reason for the small number of interviews was that there were not more participants that had volunteered to take part in the interviews from Study one and answered the invitation email for booking an interview time. Interviews could have been performed also with participants from Study two, but time became a restraint at that point in time.

6.3.5. Questionnaires

One thing that could have been done better in the questionnaires is that some questions could have been framed better. One example of that is the question in Study one on if the organization had pursued vulnerabilities through legal channels. In that question, the author of this thesis meant that the organization had pursued the reporter of a vulnerability through legal channels, but the phrasing in the question does not make that completely clear. The usage of terms could also have been

clearer from the beginning, for example vulnerability reward program was also used in the questionnaire in addition to vulnerability reporting program. Vulnerability reward program is another term for a BBP. Keeping in mind how each question in the questionnaire is related to the research questions is also very important, so that the questions ask about those items that the thesis seeks to answer. This also connects with keeping the questionnaires as short as possible, as in the questionnaire, there should only be questions that help in answering the research questions. Keeping in mind the knowledge level of the group that the questionnaire is going to be answered by is also important, as if the questions ask about things that the participants do not have knowledge of, the quality of data is going to be lowered.

7. Summary and Outlook

This chapter summarizes the studies that were conducted to answer the three research questions. Finally, possible future research that is enabled by this thesis is outlined.

7.1. Summary

Two studies were performed to answer what the state of Vulnerability reporting programs (VRPs) is in Iceland, to find out what barriers affect the use of VRPs and how commonly penetration testing and system scanning are used in Iceland. A search for related work did not reveal any other study that did this for Iceland; therefore, the work described in this thesis can be considered the first study of this kind.

In Study one, upper management and cybersecurity professionals were asked questions on cybersecurity practices and VRPs through a questionnaire. From that questionnaire, 31 data points were acquired from a group that was composed mostly of upper management. Three interviews were also performed to ask further on the questions in the questionnaire and the information from them was used to give insights into the answers from the questionnaire.

In Study two, a wider group of IT professionals were asked questions on cybersecurity practices and VRPs through a questionnaire that was shorter than the one in Study one. From this questionnaire 59 data points were acquired and the group of participants was mostly IT professionals, for a big part software developers.

The first research question asked what the state of VRP is in Iceland. The outcome of this question was that the knowledge level of VRPs and BBPs is low (In Study one, 25% have a VRP and in Study two, 15% say they have one). The knowledge level of how to handle vulnerabilities that get reported was though good.

The second research question asked what the barriers were that affected the use of VRPs. The answer obtained for this question was the knowledge level on VRPs is

7. Summary and Outlook

low. As an example, in Study one 45% of participants knew a VRP platform, and only 26% knew one in Study two. It is hard to use something if one does not know much about it. Furthermore, VRPs are resource extensive for organizations who want to have one and this might prove a hurdle for the small sized companies in the Icelandic market.

The third research question asked how commonly penetration testing and system scanning is used in Iceland. What could be seen through the research in this thesis is that most (78% in Study one and 86% in Study two) organizations do regular system scanning but only around half (52% in Study one) or less (40% in Study two) perform regular penetration testing. Half of organizations being penetration tested is though better than the international average (31.7%) as can be seen in the Chapter 3.

One way to solve the problem of how resource extensive VRPs are for organizations, would be to create a national VRP for Iceland that is free for organizations to take part in that also takes care of validation vulnerability reports. Another barrier is that the increased attention that a VRP can give to systems may be dangerous for sensitive systems. For some sensitive systems, a private BBP would perhaps be suitable. Another barrier would be the lack of reporting channels which cybersecurity experts can report vulnerabilities through along with the risk of legal complications from reporting a vulnerability. These problems for the reporters of vulnerabilities would be solved if there is a clear and safe way through which to report vulnerabilities, such as a national VRP.

7.2. Outlook

The data that was obtained in the two studies described in this thesis could be further analysed. One way would be to look further into the differences between demographic groups in and between the questionnaires. This would allow drawing conclusion of what to keep in mind for the creation of VRP law for Iceland from the perspective of a cybersecurity expert. Another possible conclusion would be about how a nation-wide VRP could be created for Iceland. The use of private BBPs for sensitive systems in Iceland along with suggestions and a trial in a willing organization would also be a possible future work.

Cybersecurity culture and penetration testing in Iceland in general are subjects that could be researched more extensively. A few ideas would be to research cybersecurity culture and penetration testing in different industries in Iceland, looking into the difference between the industry and government. It would additionally be interesting to look into cybersecurity culture surrounding the interactions with critical

infrastructure along with how it is penetration tested.

Another use of this research is that it can be used as a starting point for creating a national VRP and an analysis of gaps in cybersecurity in Iceland. This relates directly to the forthcoming European Commission-funded Digital Europe Programme (DEP) projects Defend Iceland (ICEDEF) and the National Coordination Centre Iceland (NCC-IS) for cybersecurity that start in autumn 2023.

References

- [1] Alexandra Líf Arnarsdóttir et al. “Cybersecurity Maturity: Researching managerial views to develop a maturity model and cybersecurity health certificate”. Bachelor’s thesis. Reykjavik University, May 2022. URL: <http://hdl.handle.net/1946/41735>.
- [2] Erica Azad. *Inside the Mind of a Hacker: 2023 Edition*. 2023. URL: <https://ww1.bugcrowd.com/inside-the-mind-of-a-hacker-2023/> (visited on 07/25/2023).
- [3] Bandar Abdulrhman Bin Arfaj, Shailendra Mishra, and Mohammed AlShehri. “Efficacy of Unconventional Penetration Testing Practices”. In: *Intelligent Automation and Soft Computing* 31.1 (2022), pp. 223–239. ISSN: 1079-8587. DOI: 10.32604/iasc.2022.019485.
- [4] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. “Cyber Scanning: A Comprehensive Survey”. In: *IEEE Communications Surveys and Tutorials* 16.3 (2014), pp. 1496–1519. ISSN: 1553-877X. DOI: 10.1109/SURV.2013.102913.00020.
- [5] Global Cyber Security Capacity Centre. *Cybersecurity Capacity Reviews Republic of Iceland*. 2018. URL: https://www.stjornarradid.is/library/02-Rit--skyrslur-og-skrar/Cybersecurity_Capacity_Review_Iceland_Loka%C3%BAtg%C3%A1fa.pdf.
- [6] Cristina Del-Real and María José Rodríguez Mesa. “From black to white: the regulation of ethical hacking in Spain”. In: *Information & Communications Technology Law* 32.2 (2023), pp. 207–239. DOI: 10.1080/13600834.2022.2132595. eprint: <https://doi.org/10.1080/13600834.2022.2132595>. URL: <https://doi.org/10.1080/13600834.2022.2132595>.
- [7] World Economic Forum. *Global Risks Report 2023*. 2023. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.
- [8] Edwin Foudil and Yakov Shafranovich. *A File Format to Aid in Security Vulnerability Disclosure*. 2022. URL: <https://www.rfc-editor.org/rfc/rfc9116> (visited on 09/24/2023).
- [9] Google. *Google and Alphabet Vulnerability Reward Program (VRP) Rules*. URL: <https://bughunters.google.com/about/rules/6625378258649088/google-and-alphabet-vulnerability-reward-program-vrp-rules> (visited on 09/24/2023).

References

- [10] Government of Iceland Ministry of Higher Education Science and Innovation. *Icelandic National Cybersecurity Strategy 2022–2037*. 2022. URL: <https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar--og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022-2037.pdf>.
- [11] HackerOne. *Hacker-Powered Security Report 2022*. 2022. URL: <https://www.hackerone.com/resources/reporting/6th-annual-hacker-powered-security-report>.
- [12] HackerOne. *The 2021 Hacker Report - Understanding Hacker Motivations, Development and Outlook*. 2021. URL: <https://www.hackerone.com/sites/default/files/2021-03/the-2021-hacker-report.pdf>.
- [13] International Telecommunication Union. *Global Cybersecurity Index 2020*. 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.
- [14] Uldis Ķinis. “From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach”. In: *Computer Law & Security Review* 34.3 (2018), pp. 508–522. ISSN: 0267-3649. DOI: <https://doi.org/10.1016/j.clsr.2017.11.003>. URL: <https://www.sciencedirect.com/science/article/pii/S0267364917303606>.
- [15] Dominik Leiner and Stefanie Leiner. *SoSci Survey*. Version 3.3.01. 2022. URL: <https://www.soscisurvey.de>.
- [16] Tamara Lopez et al. “Security Responses in Software Development”. In: *ACM Trans. Softw. Eng. Methodol.* 32.3 (Apr. 2023). ISSN: 1049-331X. DOI: 10.1145/3563211. URL: <https://doi.org/10.1145/3563211>.
- [17] Suresh S. Malladi and Hemang C. Subramanian. “Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations”. In: *IEEE Software* 37.1 (Jan. 2020), pp. 31–39. ISSN: 0740-7459. DOI: 10.1109/MS.2018.2880508.
- [18] Tim Menzies et al. “Are Delayed Issues Harder to Resolve? Revisiting Cost-to-Fix of Defects throughout the Lifecycle”. In: *Empirical Softw. Engg.* 22.4 (Aug. 2017), pp. 1903–1935. ISSN: 1382-3256. DOI: 10.1007/s10664-016-9469-x. URL: <https://doi.org/10.1007/s10664-016-9469-x>.
- [19] National Telecommunications and Information Administration Awareness and Adoption Group. *Vulnerability Disclosure Attitudes and Actions*. 2016. URL: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

- [20] Irum Rauf et al. “Influences of Developers’ Perspectives on Their Engagement with Security in Code”. In: *Proceedings of the 15th International Conference on Cooperative and Human Aspects of Software Engineering*. CHASE ’22. Pittsburgh, Pennsylvania: Association for Computing Machinery, 2022, pp. 86–95. ISBN: 9781450393423. DOI: 10.1145/3528579.3529180. URL: <https://doi.org/10.1145/3528579.3529180>.
- [21] Ita Ryan, Utz Roedig, and Klaas-Jan Stol. “Measuring Secure Coding Practice and Culture: A Finger Pointing at the Moon is not the Moon”. In: *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. 2023, pp. 1622–1634. DOI: 10.1109/ICSE48619.2023.00140.
- [22] Joanna E. M. Sale, Lynne H. Lohfeld, and Kevin Brazil. “Revisiting the quantitative-qualitative debate: Implications for mixed-methods research”. In: *Quality and Quantity* 36.1 (Feb. 2002), pp. 43–53. ISSN: 0033-5177. DOI: 10.1023/A:1014301607592.
- [23] Mikhail A. Shlyakhtunov. “White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies”. English. In: *International Journal of Advanced Computer Science and Applications* 12.8 (2021). URL: <https://www.proquest.com/scholarly-journals/white-grey-black-hat-hackers-role-world-russian/docview/2655113348/se-2>.
- [24] Murugiah Souppaya and Karen Scarfone. *Technical Guide to Information Security Testing and Assessment*. 2008. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152164.
- [25] Christopher Sprague and Jeffrey Wagner. “Economic motivations for software bug bounties”. In: *Economics Bulletin* 38.1 (2018), pp. 550–557. URL: <https://ideas.repec.org/a/ebl/ecbull/eb-17-01024.html>.

A. Appendix

This appendix provides the full list of questions from ScoSci Survey that were used in the questionnaires of Study one and Study two, as well as the script for the questions asked in the interviews as part of Study one.

A.1. Study one questionnaire

On the following pages, the ScoSci Survey online questions used in Study one are provided.

Survey for Cyber security and Vulnerability Disclosure

Informed Consent

Research project:

The State of Vulnerability Disclosure in Iceland

Researcher investigator:

Þorsteinn Kristinn Ingólfsson, M.Sc. Student in Software Engineering at University of Iceland

Contact Information

If you have any questions about the survey or your participation, please feel free to ask the researchers at any time before, during or after the survey.

Þorsteinn Kristinn Ingólfsson, Email: thi35@hi.is

Under the supervision of:

Gerardo Reynaga, PhD

Theodor Gislason, CTO, Syndis

Helmut Wolfram Neukirchen, Professor of Computer Science and Software Engineering, University of Iceland

Matthias Book, Professor of Software Engineering, University of Iceland

Purpose of the Research

Vulnerability disclosure is the process of openness and transparency among security researchers, product and security vendors, and other stakeholders.

The intent of the research is to compile empirical data regarding vulnerability disclosure practices.

The study will contribute to understanding, improving and creating a framework for Vulnerability Disclosure and Bug Bounty programs in Iceland.

Collected Data and Confidentiality

By continuing to the next page, you agree to the following:

- Access to the survey data will be limited to research purposes only. That is the researcher, collaborators in the research process and researchers in further connected research.
- The answers from the survey will be analysed by the researcher investigator and academic colleagues and researchers with whom he might collaborate as part of the research process.
- All data collected during the experiment will be pseudonymized (i.e. associated with a neutral identification number instead of your name or affiliation), so it is not traceable to you or your organization. Parts of the pseudonymized data may be published in individual or aggregate form. If you want an follow up interview, there is though an option to link contact information to your answers. In that case your answers are not pseudonymized.
- Any summary content, or direct quotations from the survey or interview, that are made available through academic publication or other outlets will be anonymized so that you or your company cannot be identified, and care will be taken to ensure that other information in the interview that could identify you or your company is not revealed.

If agreed upon, the survey will be followed by an interview.

Refusal or Withdrawal

You have the right to refuse to participate in this survey or to leave and delete your data at any time without giving a reason, and without incurring any negative consequences. If you pause the survey but don't delete the data, the collected data can be used in the research. Once the survey is submitted, you may not forbid the use of data or demand that it be destroyed.

Incentives

There are no rewards, payments, prizes or other incentives for participation.

INFORMED CONSENT

I have understood the above information and consent to participate in this study.

Terms used in the survey

Vulnerability – A security vulnerability or threat that can adversely affect an organization

Vulnerability Disclosure – The disclosure either public or private of a security threat or vulnerability

BBP – Bug Bounty Program

VRP – Vulnerability Reward Program

Independent Researcher – white hat or grey hat hacker

White hat hackers – ethical hackers or independent security researchers who are authorised by an organisation to identify security vulnerabilities

Grey hat hackers – hackers that are not authorised by the organization to identify security vulnerabilities

Disclosee- the person that disclosed a vulnerability

Demographic Information / Tell us about your organization

1. What is the number of employees in your company?

- ☐ 1-20
- ☐ 21-50
- ☐ 51-100
- ☐ 101-500
- ☐ 501-1000
- ☐ >1000
- ☐ Do not know / Do not want to answer

2. What is the business/operations reach of your company?

- ☐ National
- ☐ European
- ☐ International
- ☐ Do not know / Do not want to answer

3. What is the organization's main focus? (Select those that apply)

- ☐ Web services
- ☐ IoT devices
- ☐ Industrial equipment
- ☐ Finance
- ☐ Retail
- ☐ Public Administration
- ☐ Education
- ☐ Other
- ☐ Do not know / Do not want to answer

4. What is the age of your company?

- ☐ <5 years
- ☐ 5-10 years
- ☐ 11-15 years
- ☐ >16 years
- ☐ Do not know / Do not want to answer

5. Does your organization have a dedicated Information Security team?

- ☐ Yes- Internal security team (One or more people)
- ☐ Yes- External security team
- ☐ No
- ☐ Do not know / Do not want to answer

6. What is your role in your organization?

- ☐ CEO
- ☐ CTO
- ☐ CISO
- ☐ Upper management
- ☐ Project Manager/Team leader
- ☐ Developer/Programmer
- ☐ Security professional
- ☐ Researcher/Professor
- ☐ Student
- ☐ Other
- ☐ Do not know / Do not want to answer

General security awareness

7. Is your company scanned for vulnerabilities on a regular basis?

(Scans requested by the company, not unwanted scans from hackers.)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

8. Is your company penetration tested on a regular basis?

(Penetration Testing is the method to evaluate the security of an application or network by safely exploiting any security vulnerabilities present in the system. This can be done by the company itself or a 3rd party.)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

9. Does your company have application security assessments?

(Application security assessments are when security professionals go over your application and check exploitable security risks, provide actionable steps to resolve those risks and make sure that the application is compliant with cybersecurity laws.)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

10. Does your company require that IT Staff are trained in software security? (either by in-house or external training)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

Vulnerability Awareness / Vulnerability Disclosure Practices

11. To which extent do you agree to these statements? (Only mark one option for each statement)

(Vulnerability Disclosure Practices are the practices used when a vulnerability is disclosed to a company/organization and how a company handles the disclosure.)

	Completely disagree	Somewhat disagree	Neither agree/disagree	Somewhat agree	Completely agree	Do not know / Do not want to answer
My organization is aware of vulnerability disclosure practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organization is aware of vulnerability disclosure practices and has done something about it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organization has looked at how other organizations are handling vulnerability disclosures.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organization has looked into best practices and/or standards.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

12. Which Vulnerability Reward Programs (VRPs) are you aware of, if any? (select all that apply)

- ☐ HackerOne
- ☐ BugCrowd
- ☐ Intigriti
- ☐ Other
- ☐ Not aware of any reward program
- ☐ Do not know / Do not want to answer

13. Does your organization have a vulnerability disclosure program?

(Vulnerability Disclosure Program is an initiative that sets out to open up a way to disclose vulnerabilities in a secure way. Companies detail their rules and policy on the disclosures of vulnerabilities, that is what is allowed and how the disclosures should be reported. This initiative can be externally or internally hosted and with or without rewards.)

- ☐ Yes
- ☐ No

No Vulnerability Disclosure Program

If your organization has a vulnerability disclosure program, then you can skip this page.
VRP stands for Vulnerability Reward Program.

14. Has the company considered creating and implementing a VRP?

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

15. What are the barriers or reasons for not implementing a VRP?

- ☐ We have other pressing priorities
- ☐ We do not house or have access to the required expertise (e.g. law makers)
- ☐ Having a VRP would be a financial burden at the moment
- ☐ We do not know much about vulnerability disclosure practices
- ☐ We would like to have a program in place but we don't have the resources
- ☐ Our development cycles are not suited for implementing a VRP
- ☐ There are legal barriers
- ☐ Other barriers
- ☐ Do not know / Do not want to answer

16. Are there any specific persons that act as barriers to implementing a VRP?

(Answer with role of person, choose one or many.)

- ☐ CEO
- ☐ CTO
- ☐ Project Manager
- ☐ Chief of Security
- ☐ Security Officer
- ☐ Other roles
- ☐ Do not know / Do not want to answer

17. Would the company be interested in implementing a VRP?

- ☐ Yes
- ☐ No
- ☐ Maybe
- ☐ Do not know / Do not want to answer

18. Do you have a timeline for implementing a VRP?

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

19. Do you have a preference for a VRP program?

- ☐ Yes- Self hosted
- ☐ Yes- third party
- ☐ Yes- other
- ☐ No
- ☐ Do not know / Do not want to answer

20. If your company does not identify benefits of implementing a VRP, why is that?

- ☐ Does not trust it
- ☐ Other
- ☐ Do not know / Do not want to answer

The organization has a Vulnerability Disclosure Program

If your organization does not have a vulnerability disclosure program, then you can skip this page.

21. What kind of vulnerability disclosure practices does your company have? (Select all that apply)

- ☐ Self-hosted Vulnerability Disclosure Program with a page detailing the program and policy (the program does not offer a reward)
- ☐ We handle our own Vulnerability Reward Program (VRP) with resources to investigate, triage, and resolve reported vulnerabilities (the program does offer a reward)
- ☐ A contact email for reporting vulnerabilities
- ☐ We have a Vulnerability Reward Program (VRP) with a third party service
- ☐ We inform and coordinate with other vendors that may be impacted by vulnerabilities reported to us
- ☐ We acknowledge reporters of vulnerabilities if they want that recognition
- ☐ We alert our consumers about fixed vulnerabilities as well as whether we do not fix (discontinued or unsupported products)
- ☐ Do not know / Do not want to answer

22. Tell us why or what prompted the organization to create and follow disclosure practices (select all that apply)

- ☐ Our organization houses the required expertise to create a program
- ☐ A Vulnerability Reward Program (VRP) in combination with pen-testing service ensures a more secure service or product for our customers
- ☐ Vulnerability Reward Program (VRP) platforms greatly facilitate having a disclosure program
- ☐ We benefit more having a Vulnerability Disclosure Program (VDP) than not having one
- ☐ Having a Vulnerability Reward Program (VRP) is cheaper and more effective than having a pen-testing service
- ☐ We are concerned about liability
- ☐ Regulations demand we have a program
- ☐ Our customers care about security as well as we do
- ☐ Our organization had an embarrassing disclosure incident which prompted us to have a program
- ☐ Other reasons
- ☐ Do not know / Do not want to answer

Disclosures to the organization

23. Has your organization received any disclosures in the last 3 years?

- ☐ Yes – from a penetration testing service
- ☐ Yes – from an independent grey hat researcher
- ☐ Yes – from an independant white hat researcher with authorization from the company
- ☐ Yes – from a Vulnerability Reward Program (VRP) platform
- ☐ Yes – from our self-managed Vulnerability Reward Program (VRP)
- ☐ No
- ☐ Do not know / Do not want to answer

Disclosures to the organization, had disclosures.

24. Has the organization pursued vulnerability disclosures through legal chanel?

(Such as seeking legal advice and pursuing legal action against the disclosee)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

25. In general, has the company been satisfied with the quality of the report(s) submitted?

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

26. Did the disclosure lead to a fix?

- ☐ Yes
- ☐ No
- ☐ There were no disclosures
- ☐ Do not know / Do not want to answer

Wording in VRPs

27. What is the best term in Icelandic for a VRP (Vulnerability Reporting Program) ?

- ☐ Suggestion
- ☐ Do not know / Do not want to answer

28. What is the best term in Icelandic for a person who looks for and reports vulnerabilities, for use in a VRP (Vulnerability Reporting Program) ?

- ☐ Suggestion
- ☐ Do not know / Do not want to answer

29. What is the best term in Icelandic for the search of vulnerabilities, for use in a VRP (Vulnerability Reporting Program) ?

- ☐ Suggestion
- ☐ Do not know / Do not want to answer

Benefits of VRP

30. To which extent do you agree to these statements?

	Completely disagree	Somewhat disagree	Neither agree/disagree	Somewhat agree	Completely agree	Do not know / Do not want to answer
It is/would be currently beneficial for my company to make use of Vulnerability Reward Programs (VRPs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pentesting is more beneficial than a VRP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A VRP would negatively expose the company	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Setting up a VRP program would be too demanding on the company at the moment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

31. What would be the best recognition for your company for having a VRP (Vulnerability Reporting Program)?

- ☐ Be on a list of companies in a program on the page of the program
- ☐ Get a badge for taking part in a program
- ☐ Do not want any special recognition
- ☐ Want to be as anonymous as possible
- ☐ Other
- ☐ Do not know / Do not want to answer

32. Do you want to participate in a follow up interview?

- ☐ Yes, and I want my survey answers to be connected to my contact information
- ☐ Yes, but I don't want my survey answers to be connected to my contact information
- ☐ No

This is the last page of the survey. When you click "Next" on this page, you won't be able to go back to the survey anymore.

Participation in a follow up interview

We would like to invite you to have a follow up interview. In the interview we would talk in further detail about vulnerability disclosure and security.

Your answers will be connected to your contact information and then your answers are not anonymized until after the interview when we delete your contact information from the data.

If you do not want to have a follow up interview, do not leave your contact information in the input.

33. Please fill this form to leave your contact info

Contact info

Email

Name

Participation in a follow up interview

We would like to invite you to have a follow up interview. In the interview we would talk in further detail about vulnerability disclosure and security.

Your contact information will not be connected to your answers so the answers stay anonymized. This means though that your answers can not be used in the interview as they can not be identified.

If you do not want to have a follow up interview, do not leave your contact information in the input.

To sign up for an interview, please fill out the following form:

[Google forms](#)

Thank you for completing this questionnaire!

We would like to thank you very much for helping us.

Your answers were transmitted, you may close the browser window or tab now.

A.2. Study one interview script

On the following pages, the interview script used in Study one is provided.

Start by asking if they want to have the interview in English or Icelandic

English version:

Introduction

We wanna begin with thanking you for participating in this interview, it is very important for our research.

The interview will go further into your views on vulnerability reporting and how it is handled in your company. The purpose is to gather data on the views of participants on specific topics from the survey. The interview will help with increasing knowledge and understanding around vulnerability reporting and how that should be done in the Icelandic market.

The interview will be recorded if you are alright with that. The data from the interview will only be used by the researchers and will be deleted when the research is over. We will be able to take anonymous and indirect quotes from the recording and aggregate its content to the research.

The interview should take 40 minutes.

Deep dive into some of the questions from the survey

1. What do you think about your organization's vulnerability disclosure practices?
2. Would the company be interested in implementing a VRP? / Has the company considered creating and implementing a VRP?
3. What are the barriers or reasons for not implementing a VRP?(talk about listed barriers of interviewee and go from there)
 - a. Explore the financial, human resource, lack of know-how, competing priorities, triage and reward compensation, company culture
4. (If the organization has implemented disclosure practices/has bug bounty) Tell us why or what prompted the organization to create and follow disclosure practices (select all that apply)
 - a. Explore

5. Has your company received disclosures?
 - a. How did the process of disclosing go?
 - b. Did the disclosure lead to a fix?
Was it a serious vulnerability?
 - c. Was it taken seriously within the company?
 - d. Do you think it should have been handled differently?
6. It happens that companies pursue legal action against those that disclosed vulnerabilities like in a well known school system that went into the news because of a vulnerability. Has anything similar happened in your company or a company you have worked for? (Such as seeking legal advice and pursuing legal action against the discloser)
7. What do you think would be the best way to give recognition to the company for having a VRP(list of companies in it, badge, non needed).
8. Is your company penetration tested on a regular basis?(change to ask about frequency and reasons, type)
 - a. Do you think that is important?
9. How are staff trained in software security in your company?
10. Does your company keep up with reported vulnerabilities and their resolution in systems and products you use?
 - a. What about vulnerabilities in your production systems, do you update them?
11. What would be a good term in Icelandic for VRP and the reportee (cyber security researcher)?

Is there anything you would like to add?

Icelandic version:

Inngangur

Við viljum byrja á að þakka þér kærlega fyrir að taka þátt í þessu viðtali, það er mjög mikilvægt fyrir þessa rannsókn.

Viðtalið mun fara nánar út í álit þitt á tilkynningum veikleika sem og hvernig því er háttað í þínu fyrirtæki/þeim fyrirtækjum sem þú hefur starfað. Tilgangur viðtalsins er að safna gögnum um álit þáttakenda nánar á ákveðnum málefnum úr spurningakönnuninni. Það mun aðstoða við að auka þekkingu og skilning í kringum tilkynningarkerfi veikleika og hvernig þau eiga að vera uppsett á íslenskum markaði.

Viðtalið verður hljóðritað ef þú ert sátt/sáttur með það. Gögnin úr viðtalinu verða aðeins notuð af rannsóknarmönnum og verður eytt þegar rannsókn er lokið. Við getum tekið nafnlausar og óbeinar tilvitnanir út frá hljóðrituninni og glósum úr viðtalinu og notað það í rannsókninni.

Viðtalið ætti að taka í kringum 40 mínútur.

Deep dive into some of the questions from the survey

1. Hvað finnst þér um starfshætti í tilkynningum veikleika í þínu fyrirtæki?
2. Myndi fyrirtækið hafa áhuga eða hugsað um það að koma af stað eða vera hluti af tilkynningagátt veikleika?
3. Hverjar eru hindranir í að koma af stað tilkynningagátt veikleika? (t.d. fjárhagslegt, mannauður, þekking, forgangsörðun, tjóna og umbunarbætur, fyrirtækjamenning)
4. (Ef hefur búið til tilkynningagátt) Segðu mér nánar frá ástæðunum fyrir því að fyrirtækið bjó til og fara eftir tilkynningastarfsháttum.
5. Hefur fyrirtæki sem að þú hefur unnið hjá fengið tilkynningu veikleika?
 - a. Hvernig gekk ferlið fyrir tilkynninguna?
 - b. Leiddi hún til lagfæringar?
 - c. Var veikleikinn alvarlegur?
 - d. Var veikleikanum tekið alvarlega í fyrirtækinu?
 - e. Finnst þér að eitthvað hefði mátt vera gert öðruvísi?
6. Það kemur fyrir að fyrirtæki kæri þá sem að tilkynna veikleika í kerfum eins og gerðist hjá vel þekktu skólakerfi á Íslandi og kom fram í fréttum á sínum tíma. Hefur eitthvað álíka komið upp hjá fyrirtæki sem að þú hefur unnið fyrir?
7. Hvert finnst þér að væri besta leiðin til þess að veita fyrirtækjum viðurkenningu fyrir að hafa eða taka þátt í tilkynningargátt? (badge, listi yfir fyrirtæki sem að taka þátt, þarf ekki)
8. Er fyrirtækið þitt penetration testað reglulega?

- a. Finnst þér það mikilvægt?
- 9. Hvernig er starfsfólk þjálfað í stafrænu öryggi í þínu fyrirtæki?
- 10. Does your company keep up with reported vulnerabilities and their resolution in systems and products you use?
- 11. Fylgist þitt fyrirtæki með tilkynningum veikleika og úrlausn þeirra í kerfum/vörum sem að þið notið?
 - a. Hvað með veikleika í rekstrarkerfum, uppfærið þið þau?
- 12. Hvað væri gott orð yfir Bugbounty eða tilkynningagátt veikleika á íslensku?(Skoða svör frá þeim)

Hefurðu eitthvað sem þú myndir vilja bæta við?

A.3. Study two questionnaire

On the following pages, the ScoSci Survey online questions used in Study two are provided.



The State of Vulnerability Disclosure in Iceland

Researcher:

Þorsteinn Kristinn Ingólfsson, M.Sc. Student in Software Engineering at University of Iceland
Any questions about the survey can be sent to Email: thi35@hi.is.

Purpose of the Research

The purpose of the research is to compile data about the culture and practices in companies around receiving information about faults in their systems and how they can be exploited (vulnerability disclosing). Furthermore the research will contribute to understanding, improving and creating a framework for Vulnerability Disclosure and Bug Bounty programs in Iceland.

Collected Data and Confidentiality

By continuing to the next page, you consent to the following:

- Access to the survey data will be limited to the researcher, collaborators in the research process and researchers in further connected research. The answers from the survey will be analyzed by the aforementioned as part of the research process.
- Data collected in the survey is pseudonymized (i.e. associated with a neutral identification number instead of your name or affiliation), so it is not traceable to you or your organization. Care will be taken to ensure that information that could identify you or your company is not revealed. Parts of the pseudonymized data may be published in individual or aggregate form.

Refusal or Withdrawal

You have the right to refuse to participate in this survey or to leave and delete your data at any time without giving a reason, and without incurring any negative consequences. If you pause the survey but don't delete the data, the collected data can be used in the research. Once the survey is submitted, you may not forbid the use of data or demand that it be destroyed.

There are no rewards, payments, prizes or other incentives for participation.

1. What is the number of employees in your organization?

- ☐ 1-20
- ☐ 21-50
- ☐ 51-100
- ☐ 101-500
- ☐ >500
- ☐ Do not know / Do not want to answer

2. What is the business/operations reach of your organization?

- ☐ National
- ☐ European
- ☐ International
- ☐ Do not know / Do not want to answer

3. What is the organization's main focus? (Select those that apply)

- ☐ Web services
- ☐ IoT devices
- ☐ Industrial equipment
- ☐ Finance
- ☐ Retail
- ☐ Public Administration
- ☐ Education
- ☐ Other
- ☐ Do not know / Do not want to answer

4. What is the age of your organization?

- ☐ <5 years
- ☐ 5-10 years
- ☐ 11-15 years
- ☐ >16 years
- ☐ Do not know / Do not want to answer

5. What is your role in your organization?

- ☐ Project Manager/Team leader
- ☐ Developer/Programmer
- ☐ Security professional
- ☐ Researcher/Professor
- ☐ Student
- ☐ Other
- ☐ Do not know / Do not want to answer

6. Does your organization have a dedicated Information Security team?

- ☐ Yes – Internal security team (One or more people)
- ☐ Yes – External security team
- ☐ No
- ☐ Do not know / Do not want to answer

7. Mark everything that fits with your organization

(Penetration testing: Method to evaluate the security of an application or network by safely exploiting any security vulnerabilities present in the system.)

- ☐ My organization is scanned for vulnerabilities on a regular basis (requested by the company)
- ☐ My organization is penetration tested on a regular basis
- ☐ My organization has application security assessments
- ☐ My organization requires that IT Staff are trained in software security (in-house or external training)

8. Mark everything that fits with your organization

(Vulnerability Disclosure Program (VDP): Organizations detail their rules and policies on the disclosures of vulnerabilities. That is, what is allowed and how the disclosures should be reported. Vulnerability Reward Program (VRP): VDP with rewards for vulnerabilities found.)

- ☐ My organization has a vulnerability disclosure program
- ☐ My organization has considered creating and implementing a VRP
- ☐ My organization is interested in implementing a VRP
- ☐ My organization has a timeline for implementing a VRP
- ☐ Do not know / Do not want to answer

9. To which extent do you agree to these statements?

(Vulnerability Disclosure Practices are the practices used when a vulnerability is disclosed to a company/organization and how an organization handles the disclosure.)

	Completely disagree	Somewhat disagree	Neither agree/disagree	Somewhat agree	Completely agree	Do not know / Do not want to answer
My organization is aware of vulnerability disclosure practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organization and has done something about its vulnerability disclosure practices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organization has informed itself on best practices and how other organizations are handling disclosures.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
It is/would be beneficial for my organization to make use of Vulnerability Reward Programs (VRPs)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pentesting is more beneficial than a VRP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

10. Which Vulnerability Reward Program (VRP) platforms are you aware of, if any? (select all that apply)

- ☐ HackerOne
- ☐ BugCrowd
- ☐ Intigriti
- ☐ Other
- ☐ Not aware of any reward program platform
- ☐ Do not know / Do not want to answer

11. Has your organization received any disclosures in the last 3 years? (select all that apply)

(White hat hackers: ethical hackers or independent security researchers who are authorized by an organisation to identify security vulnerabilities. Grey hat hackers: hackers that are not authorized by the organization to identify security vulnerabilities)

- ☐ Yes – from a penetration testing service
- ☐ Yes – from an independent grey hat researcher
- ☐ Yes – from an independent white hat researcher with authorization from the organization
- ☐ Yes – from a Vulnerability Reward Program (VRP) platform
- ☐ Yes – from our self-managed Vulnerability Reward Program (VRP)
- ☐ No
- ☐ Do not know / Do not want to answer

12. Do you have a preference for a VRP program?

- ☐ Yes – Self hosted
- ☐ Yes – third party
- ☐ No
- ☐ Do not know / Do not want to answer

13. If you/your organization does not identify benefits of implementing a VRP, why is that? (select all that apply)

- ☐ It is complex and there's lack of expertise
- ☐ It would negatively effect the image of the organization
- ☐ Cost of the program
- ☐ Exposure of systems
- ☐ Lack of resources/takes up too much resources
- ☐ Other
- ☐ Do not know / Do not want to answer

14. Has the organization pursued vulnerability disclosures through legal channels?

(Such as seeking legal advice and pursuing legal action against the disclosee)

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

15. In general, has your organization been satisfied with the quality of the report(s) submitted?

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

16. Did the disclosure lead to a fix?

- ☐ Yes
- ☐ No
- ☐ Do not know / Do not want to answer

17. What are the best Icelandic translations for a VRP (Vulnerability Reporting Program)

- ☐ Tilkynningargáttveikleika
- ☐ Veikleikagátt
- ☐ Villuveiðagátt
- ☐ Öryggisgátt
- ☐ Other
- ☐ Do not know / Do not want to answer

18. What is the best term in Icelandic for a person who looks for and reports vulnerabilities, for use in a VRP ?

- ☐ Hakkari
- ☐ Öryggissérfræðingur
- ☐ Veikleikaleitari
- ☐ Veikleikarýnir
- ☐ Other
- ☐ Do not know / Do not want to answer

19. What is the best term in Icelandic for the search of vulnerabilities, for use in a VRP ?

- ☐ Veikleikaleit
- ☐ Að hakka
- ☐ Öryggisleit
- ☐ Veikleikarýni
- ☐ Other
- ☐ Do not know / Do not want to answer

20. What would be the best recognition for your organization for having a VRP (Vulnerability Reporting Program)?

- ☐ Be on a list of organization with a program on a VRP platform
- ☐ Get a badge for taking part in a program
- ☐ Do not want any special recognition
- ☐ Want to be as anonymous as possible
- ☐ Other
- ☐ Do not know / Do not want to answer

This is the last page of the survey. When you click "Next" on this page, you won't be able to go back to the survey anymore.

Thank you for completing this questionnaire!

We would like to thank you very much for helping us.

Your answers were transmitted, you may close the browser window or tab now.

B.Sc. Þorsteinn Kristinn Ingólfsson – 2021