# VICTORIA UNIVERSITY OF WELLINGTON
## *Te Whare Wānanga o te Ūpoko o te Ika a Māui*



# School of Engineering and Computer Science
## *Te Kura Mātai Pūkaha, Pūrorohiko*

PO Box 600
Wellington
New Zealand

Tel: +64 4 463 5341
Fax: +64 4 463 5045
Internet: office@ecs.vuw.ac.nz

# Why Do Programmers Do What They Do?
# A Theory of Influences on Security Practices

Lavanya Sajwan

Supervisors: James Noble, Craig Anslow

Submitted in partial fulfilment of the requirements for
Bachelor of Engineering with Honours in Software
Engineering.

## Abstract

Technologies are continually adapting to match ever-changing trends, and as this occurs, new vulnerabilities are exploited by malignant attackers and can cause significant economic damage to companies. Programmers are therefore repeatedly having to expand their knowledge and skills to protect software. Programmers do make mistakes, and this is why we must understand the thinking behind their decisions and influences to interpret how they implement and adopt security practices. Understanding these decisions can help inform design and educational decisions around improving programming language security. This report will cover the full progress of the project "Why Do Programmers Do What They Do? A Theory of Influences on Security Practices"

# Acknowledgements

I would like to thank my supervisors James Noble and Craig Anslow for their ongoing support and direction as I have completed this project.

To dad and mum, thanks for harassing friends to potentially participate in this study. With the addition of my brother; thank you for having no idea about what I have been doing all year long, but also for leaving me fairly alone for these last two weeks as I recluse into a hole where I write, write, write and write.

And to Janaye; a massive thanks for reading over this report and being my grammar and punctuation whizz since high school.

# Contents

# Chapter 1

# Introduction

As software is now ubiquitous across many industries, it is impossible to not have a presence in the tech sphere. Consequently, software security has become so significant, programmers have to ensure that the security processes that they implement are resilient to any attacks. Lack of attack prevention can cause leakage of sensitive information, major economic damage and danger to massive numbers of users and employees. Consequently, this opens businesses, clients and end-users to exploitation by external bodies. Unfortunately, every day, we hear of compromised organisations [1]. Last year New Zealand experienced a significant security breach within the Tū Ora Compass Health (Tū Ora) Primary Health Organisation (PHO) [2]. Tū Ora is one of the largest PHO's in the country, and it governs the greater Wellington region [2]. Personal information of up to one million New Zealander's was exposed, and the effects of this are ongoing [2]. Costs have been high in attempts to mitigate any effects to the public. Dedicated call centres have been set-up as well as dedicated mental health lines [3, 2]. Regular updates are released in order to maintain communication transparency and assurance quality measures are ongoing [3, 2].

Qualitative research is often neglected and overlooked in favour of more quantitative reasoning and technical traits such as the security method used or the programmers task-completion rate [4]. Programmers provide a human aspect to a technical solution and there should therefore be a shift towards understanding the more background 'soft' processes that occur when making decisions; why are the choices made based on past influences, and how do they affect the programmers work in the present?

Exploring this topic is essential as it allows for a more comprehensive understanding of how and why programmers think the way they do, and of the human and social aspects of Software Engineering [5]. We want to understand what solutions programmers are using to implement in their security practices, if at all. The findings from this study can support programmers in terms of education and the better design of security methods in programming [6] that have an emphasis on usability. The findings of this project can also be used to identify what security methods programmers find as beneficial in their programming. This will allow programmers to complete their work to a high standard, by adhering to proper security protocols, thus overall making their work of a higher value both in a secure and professional sense.

Beyond the research aspect, when security and privacy issues do occur in real-world scenarios, programmers are blamed first as it is the faults in their implementation which allow for the exploitation of vulnerabilities [7]. Programmers do make mistakes, which is why they need the support to make better security decisions, and this support is currently

lacking in the industry [7]. Education is limited past initial acceptance within organisations, and often programmers have a blasé attitude regarding security, instead expecting other teams to fix the issue [8]. Furthermore, security mechanisms often have increased complexity, which makes them challenging to understand and to then use [9].

This project will investigate how programmers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impact decisions surrounding their technical work. This project uses Grounded Theory, a method which aims to establish a theory when there is none [10], and it is commonly used for data analysis. Interviews will take place to collect the data, to then analyse and present a theory on standard security practices in the professional workplace. This project builds upon works by Hala Assal, Charles Weir and Nathan Newton [6, 1, 11].

Participants will be recruited by posting on tech-related groups (i.e. From OWASP Meetup Group and LinkedIn) and mailing lists and also using my own and my supervisor contacts. At this point, semi-structured interviewing can take place with 10-20 interested individuals on the topic of their security practices while programming. Practices include; libraries, frameworks, protocols and specific languages. These people will all be programmers in New Zealand that are in varying stages of their careers and career paths to allow for a broader range of responses and a case study relevant to New Zealand. Examples of appropriate job titles include;

- DevOps Engineer

- Software Developer

- Software Engineer

- Front-end security developer

- Database administrator

- Tester

- Security Architect

- Security Consultant.

This project will lead to a new, more in-depth understanding of the psychology of the decisions made by programmers which can support security education programmes in tertiary education providers and within the workplace. The research undertaken by this project could lead to future qualitative research on another under-developed topic on why programmers do what they do. Paired with this research, future studies could help build a profile of a programmer and their thought processes. Data collected could also be the foundation that allows a programmer to build tools that help other programmers implement proper security practices; a Grammarly for security. It can also help the further development of existing static analysis tools such as Infer developed by Facebook, Tricorder used by Google, Coverity and Raygun [12, 13, 14, 15]. These tools all work by providing security detection modules and are used for quality assurance and security.

# Chapter 2

# Background

Conceptually, this project aims to gather data in order to ultimately form a theory on the influences of security practices in New Zealand. Therefore, It is essential to know enough information about the topic of security so that interviews with professional programmers are conducted in a knowledgeable manner. This chapter will include some background on what security actually is, the importance of information security practices, widely used security practices and summaries on existing research on similar subject matter.

## 2.1 What is Security?

Three objectives define security; Confidentiality, Integrity and Availability, most commonly referred to as the CIA triad. The triad measures, controls and protects information assets which include hardware, software, firmware, information data and telecommunications **INSERT NIST CITATION**. A now common synonym for security is the term coined; cybersecurity **INSERT NIST CITATION**.

Confidentiality is the act of maintaining protection of information from threat agents **INSERT BOOK CITATION**. This term also encapsulates privacy where "individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed **INSERT BOOK CITATION**. Integrity is the maintenance of data, so that information and programs are only changed when needed by authorised bodies **INSERT BOOK CITATION**. It also covers system integrity where "a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system" **INSERT BOOK CITATION**. Availability is the act of ensuring reliable access to information to authorised users **INSERT BOOK CITATION**. Any breach of these principles can result in significant adverse impacts on reputation, health and safety, service delivery as well as finances **INSERT IMPACTS CITATION**

## 2.2 Information Security in New Zealand

A study run by Aura Security showed a 10% increase in cyber-attacks on New Zealand businesses between the years of 2018-2019 [16]. In NZ, the rise is attributed to the digitisation of day-to-day way-of-life; as new technologies continually develop, there is an urgency to deploy products. There is a lot of pressure on programmers to finalise these products, and the deviation of attention to the finished output means that there are many new threats to security [17]. Malicious attackers are also becoming more sophisticated. Individual threat

attackers now seem to have the same knowledge and resources as nation-backed threat actors [17].

Areas of improvement identified by the New Zealand government are [17]:

1. **Cyber security-aware and active citizens:** Increased regular awareness campaigns and education opportunities for the public in regards to best personal security practices.

2. **Strong and capable cybersecurity workforce and ecosystem:** Increased promotion and support of the development of the cyber industry in New Zealand.

3. **Internationally active:** Detect and prevent any breaches as well as proactively maintaining international relationships regarding information security and participating in any rule reforms.

4. **Resilient and responsive New Zealand:** Supporting infrastructure, businesses, charity organisations, community organisations, individuals in improving security capabilities and resilience.

5. **Proactively tackle cybercrime:** Increasing support to impacted parties, preventing and encouraging reporting of any cybercrimes.

These five principles are planned to continue to improve upon till 2023 [17]. It is expected that aspects of these will influence the security practices that programmers use in NZ industry.

## 2.3 Secure Programming Practices

Secure refers to protecting and deterring any security incidents due to vulnerabilities in program code **(CITE THIS)**. Without a focus on security while programming, there is a lack of confidence in the outputted security, resulting in the lack of use and waste of time, effort and money. Using unsecured programs poses significant adverse impacts to businesses and individuals.

The Open Web Application Security Project (OWASP) has outlined a checklist to ensure that code is secure. They have provided this document which spans various languages and technologies as the non-profit foundation aims to improve the security across all software. It states that it is "much less expensive to build software than to correct security issues" [18].

Significant items from the checklist include [18]:

- **Input Validation:** This is the act of validating that all inputs are trusted. Examples of inputs are data from databases, file streams, as well as client-provided data. Anything classed as 'untrusted', should fail and result in a rejection. The application should have one input validation routine, a specified standard character set and all validation should occur on a preset trusted system.

- **Output Encoding:** Data sent back the client needs to be output encoded. To make this secure, a started test routine has to be utilised, and similar to input validation; all encoding must occur on a preset trusted system.

- **Authentication and Password Management:** This is verifying whether a user is allowed to act. Best practice is restricting all resources except the ones intended to be public. All authentication controls should be able to fail in order to maintain security, and passwords need hashing. In order to pass, authentication has to occur first, and every detail has to match the protected records.

- **Session Management:** A session should only associate the same client ID. It can only occur after authentication.

- **Access Control:** Set users access based on system permissions. It should use only preset, trusted systems.

- **Cryptographic Practices:** All assets should be protected by cryptography. A policy should be established in how to manage the public and private keys.

- **Error Handing and Logging:** All application errors must be 'caught' and handled. They should not disclose any information in the error responses, and instead, only show in the logs. A few can only access the logs themselves, and mechanisms should be in place to analyse the logs.

- **Data Protection:** Protect most assets, communications and caches. Encrypt any stored information that holds significant value.

- **Communication Security:** Encrypt any communication channels. Certificates should be valid, and the protocol Transport Layer Security should be in use.

- **System Configuration:** Ensure that everything is up to date. This includes servers, frameworks, components, languages, IDE's and libraries. Remove unnecessary information before deployment; test code, TODO's, HTTP methods and response headers.

- **Database Security:** Maintain short connections. Authentication needs to be checked prior use, and access control needs to be restricted.

- **File Management:** Require authentication and access control before any interaction with files. Validate file headers. Implement safe uploading by scanning for any malicious intent; viruses and malware.

- **Memory Management:** Check buffers. If larger than expected, potentially has malware or viruses. Avoid the use of vulnerable functions - *printf, strcpy*

- **General Coding Practices:**
    - Use tested and trusted components for tasks
    - Restrict users from altering code in any way
    - Review all third party components; code and libraries
    - Initialise all variables and fields

## 2.4 Related Work

This project expands upon ideas on the following works; A Survey with Software Developers - Think secure from the beginning; and Kirk and Tempero's, Software Development in New Zealand.

### 2.4.1 "Think secure from the beginning" – Assal and Chiasson

In "A Survey with Software Developers" [6], the authors pursue to understand the human behaviours and motivations surrounding factors of software security. The authors specified a series of questions targeted toward software developers through an online survey. The research examined responses to support the professional development of programmers further, both in theory and practice. This was chosen as background reading as it aligns well with the research goals of "Why Do Programmers Do What They Do?", as it aims to form a theory on the influences and effects of decisions surrounding technical work.

The results outlined the following common groups:

1. **Work Motivation:** Developers did not lack motivation in their job. They performed based on self-determination.

2. **Understanding of software security:** Developers had a sound understanding of software security. They grasped the importance of securing technical work and the discussed various methods of doing so and specifying at what stages in the project life-cycle they should implement these based on "best practices".

3. **Security Issues:** Majority of the participants believed their software could be compromised, despite being comfortable with the approaches to protecting the software. The majority has also experienced a security issue, whether that be a breach or vulnerable code.

From these common groups, the overarching theme displayed was that the developers were not purposefully ignorant about maintaining security practices; the majority were proactive and willing to learn. However, it was the importance of functionality and lack of ongoing support from organisations which made working towards a more secure software challenging.

This paper was valuable to read as there are strong similarities between the research topic developed in this and the subject of this ENGR489 project. The methodologies are different; however, this paper's findings display a programmers personal perspective rather than a theorised view. It is a direct comparison to our project, and we can further outline questions directed to the future work stated in the article's conclusion; "to explore potential relationships between motivations, deterrents and strategies for software security" and "investigate security procedures and attitudes in companies that have experienced security breaches and compare it to others who have not".

Similar questions from the survey were used for the interview process in this study. Important questions identified are:

- How does security fit in the development life-cycle in real life?

- What are the current motivators and deterrents to developers paying attention to security?

The differences and similarities can be easier understood in the table below:

| | This Research | Assal and Chiasson's Research |
|---|---|---|
| **Data Collection** | Interview | Survey |
| **Participant Group** | Any type of programmer | Software Developers |
| **Location** | New Zealand | North America |
| **Data Type** | Confidential | Anonymous |
| **Results** | Analysis of participant answers and observations | Based on participant answers |
| **Topic** | Security | Security |

Table 2.1: Summary of comparison with "Think secure from the beginning"

### 2.4.2 "Software Development Practices in New Zealand" – Kirk and Tempero

In "Software Development Practices in New Zealand" [19], the report authors look to "developing and applying a range of software productivity techniques and tools to enhance the performance of the New Zealand software industry". Like Assal and Chiasson, the authors of this study outlined a series of questions in a survey targeted towards known Information Technology organisations. The survey aimed to understand the practices used by industry and in the findings can be used to make recommendations on best-use development practices for organisations. Kirk and Tempero's report is similar in output to the ENGR489 project as the findings can be used to make suggestions for teams adopting and developing security practices. This was chosen as a background reading as it provides insights on the current state of industry in New Zealand, which is what I aimed to develop in the research outlined in this report.

The key findings of this study were:

1. Organisations and individuals **do not follow** standard agile process models.

2. New Zealand is generally more **implementation-focused** in software development. There is an emphasis on this over other aspects of the software development life-cycle such as security and testing.

3. Decision-making is a **collaborative effort** with individuals involved in different stages and traits of the development life-cycle.

4. While most New Zealander's state they are "agile" this is not supported as frequent contact with clients and stakeholders is not upheld. However, there is a **highly iterative aspect** to the work individuals do on projects which do maintain agile principles.

5. There is a **weakness in requirements gathering** which results in a widely noticed lack of clarity on scope details.

6. This point also relates to point 2, there is a noticed severe **lack of code quality** whether this is in design, reviewing and testing stages, or with general coding best practices.

7. Most **do not develop around** tools such as libraries - rather they use them as a support. This can be derived as not being "best-practice" and can be more time-consuming.

Not much was asked specific to security, but finding number 6 links to poor practices around secure programming.

The report had a limitation in which it did not make any recommendations at this stage, but it did mention that these findings can be used by organisations to obtain a view of the software practices in New Zealand. From here, organisations can make their own decisions on what to focus on to better their specific operations.

Comparing to the described ENGR489 project, the methodology is different, and while the topics to are differing, they are similar enough to make interesting comparisons between the two. Kirk and Tempero focus on software development practices, while this project will research security practices. A comparison that can be made could be between the findings, as much like the prior related work; the findings are that of a personal perspective of the participants rather than an objective view which Grounded Theory supplies.

The differences and similarities are outlined in the table below:

| | This Research | Kirk and Tempero's Research |
|---|---|---|
| **Data Collection** | Interview | Survey |
| **Participant Group** | Any type of programmer | If developing software |
| **Location** | New Zealand | New Zealand |
| **Data Type** | Confidential | Anonymous |
| **Results** | Analysis of participant answers and observations | Based on participant answers |
| **Topic** | Security | Software Best Practices |

Table 2.2: Summary of comparison with "Software Development Practices in New Zealand"

### 2.4.3 "Challenging Software Developers: Dialectic as a Foundation for Security Assurance Techniques" - Weir, Rashid, Noble

In "Challenging Software Developers: Dialectic as a Foundation for Security Assurance Techniques"[20], the authors identify that security is more reliant on developers, but that the developers are not providing the security that is needed. Similar to the study outlined in the ENGR489 study, this was conducted using a Grounded Theory Methodology. In contrast, there were two parts of the survey, and each one was a separate grounded theory mini-study.

The authors' interview participants in order to obtain data so they can find ways to "help programmers themselves to improve security given existing constraints". This reading was chosen as it held a similar topic and was conducted using the same methodology as the ENGR489 project; Grounded Theory.

The two major findings of each survey showed:

1. Developer security is based on challenges in order to motivate better practice. These challenges are often fun adversary questioning usually to do with review and advisory. This emerged as the core theory as it was interwoven through most of the participant responses.

2. Six assurance techniques were identified in being the most helpful; threat assessment, stakeholder negotiation, configuration review, vulnerability scan, source code review and penetration testing. They all help provide software security.

These two ideas are linked, as not only do those six assurance techniques mitigate any challenges, they also provide challenges to the developer when dealing with them.

This paper was valuable to read as it provided another method of conducting grounded theory; by the use of two separate surveys that can be combined to provide their own intermingled findings. There are also similarities to the topic of this ENGR489 project. In a direct comparison to this project, where the authors outlined that they wanted to help programmers improve their security, I was initially more focused on the improvement of the technical design of security tools, frameworks and libraries.

The similarities and differences can be best understood below:

| | This Research | Weir, Rashid and Noble's Research |
|---|---|---|
| **Data Collection** | Interview | Interview x2 |
| **Participant Group** | Any type of programmer | Mobile app developers |
| **Location** | New Zealand | UK, USA, Sweden, Germany |
| **Data Type** | Confidential | Confidential |
| **Results** | Analysis of answers/observations | Analysis of answers/observations |
| **Topic** | Security | Security |

Table 2.3: Summary of comparison with "Challenging Software Developers: Dialectic as a Foundation for Security Assurance Techniques"

# Chapter 3

# Methodology

This chapter outlines the methodology that was followed to obtain findings in this study. It then deconstructs the methodology further to describe the data collection and data analysis process. The data collection subsection provides a summary of the participants.

## 3.1   Grounded Theory

Grounded Theory (GT) is the chosen methodology for this study. It was an appropriate choice as the study focuses on human aspects, and GT is a way of analysing qualitative data with the end-goal of defining a new theory from the sampled data [5]. There are several steps in the GT methodology in order to make the final theory. The theory is expected to be explanatory, focusing on describing elements of the findings rather than stating. It should also be based on the collected responses and observations, rather than pre-conceived ideas. As such, extensive literature reviews should be avoided.

Initially, researchers must choose a topic and research whether the Grounded Theory method is the right one for the research project [5]. After contacting potential participants, the iterative process of data collection occurs. Questions adapt between the rounds of the collection as the data is analysed. This refinement of questions happens to delve deeper into the traits of the emerging theory. When saturation is achieved, no further new findings are displayed which contribute to the final theory. This results in the "grounded" nature of the overall theory.

Interviews were chosen as the method of data collection as this is what is the norm in grounded theory studies [5]. Interviews are semi-structured and are more open-ended compared to the likes of a diary study or a survey. This is beneficial as it allows for participants to feel more comfortable and have more control over their answers. It also allows an interviewer to correspondingly make observations of the participant and make connections with their responses [5]. A concrete emergent theory is then formed as it is built upon two sources. This emergent theory aims to explain a practice or a phenomenon.

In the study outlined in this report, at approximately ten interviews, the concepts obtained from the data collection started to become quite similar. This is called saturation point and is when some new lower-level ideas are being obtained, but no overly new information. This was the grounding point of this specific Grounded Theory.

Initially, I aimed to get more technical empirical evidence on programmers and their se-
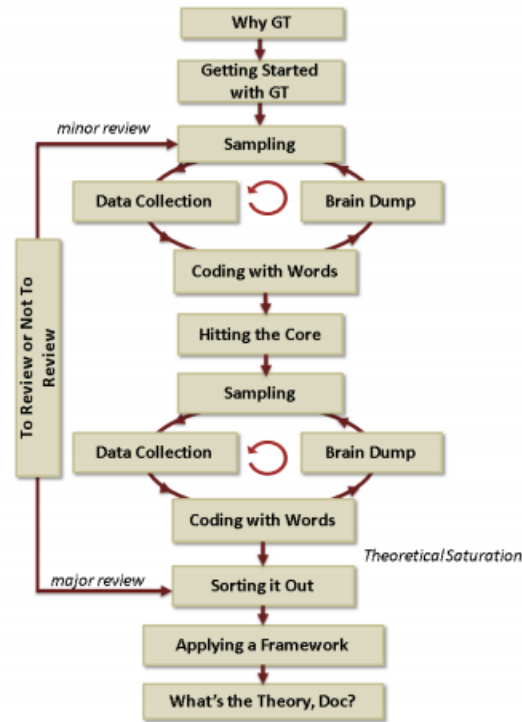
Figure 3.1: The Grounded Theory Pattern (Hoda, Noble, & Marshall, 2011)

curity practices. However, as early as the third interview, it was identified that technical security programming practices are not as influential as initial thought, and the interview questions changed to match this gradual shift in focus. This is another benefit of Grounded Theory as questions do not have to stay the same; instead, they undergo iterations of development as an area of interest. shifts.

Similar projects at the university have been conducted using this methodology. Siva Dorairaj's, "The Theory of One Team: Agile Software Development with Distributed Teams"; Rashina Hoda's, "Self-Organising Agile Teams: A Grounded Theory"; Brendan Julian's, "Agile Practices: A Theory of Agile Adoption and Evolution"; Nathan Newton's, "Information Security in Agile Software Development: A Critical Success Factor Perspective"; and Aaron Pangs, "What Programming Languages Do Developers Use? A Theory of Static vs Dynamic Language Choice" [21].

## 3.2 Data Collection

### 3.2.1 Recruitment

A recruitment post of this study supported by a webpage [22] was sent to mailing lists and websites like OWASP Meetup and LinkedIn. These are shown in Appendix E and Appendix F, respectively. There was a brief halt in the recruiting through the Meetup website as I got banned for posting in groups as I was marked as spam. However, I did not get much interest from the promotion through both Meetup and Linkedin and instead relied on personal contacts (friends and family-friends) and supervisor contacts for initial recruitment. Participants also helped with recruitment by reaching out to others in the industry and telling

them about this study.

### 3.2.2 Interviews

Fifteen interviews were agreed upon and conducted of participants across New Zealand. These participants were from fourteen unique organisations. Participants had varying job titles, years of experience, and were in a range of different sectors and organisation fields. The diversity within the participants allowed for connections to be made across a broader range of people.

Human ethics approval had to be gained before the interview process could commence. This document is displayed in Appendix B. Questions were adapted dependent on the analysis between the interviews and changed as a result of participants answers within the interview. This was so any intriguing information could be queried further during the semistructured interview. Therefore, the list of interview questions in Appendix D changed with only the "Participant Background" section remaining as a constant.

Due to the disruptive year, interviews were predominantly conducted over Zoom. Consent from the participants was obtained through an email response as per Human Ethics committee request. Interviews ran for periods ranging between 30-90 minutes. A summary of the participant sample is provided in the table below.

| Alias | Role | Experience (Years) |
|-------|------|--------------------|
| P1 | Enterprise Architect and Domain Lead | 15< |
| P2 | Principal Product Architect | 15< |
| P3 | Senior Security Architect | 10-15 |
| P4 | Senior Software Engineer | 15< |
| P5 | Software Developer | <2 |
| P6 | Level 2 Security Analyst | 2-5 |
| P7 | Site Reliability Engineer | <2 |
| P8 | DevOps Engineer | <2 |
| P9 | Portfolio Architect | 10-15 |
| P10 | Full-stack Software Developer | 2-5 |
| P11 | Cloud Engineer | 2-5 |
| P12 | Consultant (Cloud Engineering) | 2-5 |
| P13 | Development Manager and Technical Lead | 10-15 |
| P14 | Senior Software Engineer | 10-15 |
| P15 | Business Rule Consultant | 15< |

Table 3.1: Participant Aliases and Summary

## 3.3 Data Analysis

After transcribing interviews and pairing them with written observations), the selecting coding process occurs [5]. Key points from each transcript are paired with a simplified summary of the points [5]. The constant comparison method is used where codes are compared to others from within the same interview and also with other interviews [5]. These comparisons

continue to occur, and higher abstractions are found, also referred to as Axial coding **IN-SERT CITATION** . They are further narrowed to become categories for the theory [5], also referred to as Selective coding [5]. Therefore, this coding process has three key steps. Theoretical notes are written throughout this coding process to research relationships between concepts and categories [5].

# Chapter 4

# A Theory of Influences on Security Practices

This chapter will outline the emergent theory that has been found through the analysis of the findings. The three-step coding process described in the methodology section was used to achieve this theory. The three found categories will be further explained and the relationship between each of them.

### 4.0.1  Emergent Theory

The emergent theory consists of three main categories oh what influence programmers:

1. Culture in groups of individuals

2. Organisational structuring and practices

3. Industry trends

Figure 4.1: The diagram of the emergent Influences on Security Practices theory

A prior iteration of the diagram had shown one more category; "Teams". However, as the constant comparison process occurred, the factors of teams seemed to be more-so attributed to organisational structuring and practices. This meant that this category title was discarded and the factors were merged into "Organisations". Another discarded category was the influence of stakeholders. At the beginning of the interview process, clients and vendors seemed to have significant influence to the security practices implemented by programmers, but as the analysis process developed, it was not as strongly quoted in the data

# Chapter 4

# A Theory of Influences on Security Practices

This chapter will outline the emergent theory that has been found through the analysis of the findings. The three-step coding process described in the methodology section was used to achieve this theory. The three found categories will be further explained and the relationship between each of them.

### 4.0.1  Emergent Theory

The emergent theory consists of three main categories oh what influence programmers:

1. Culture in groups of individuals

2. Organisational structuring and practices
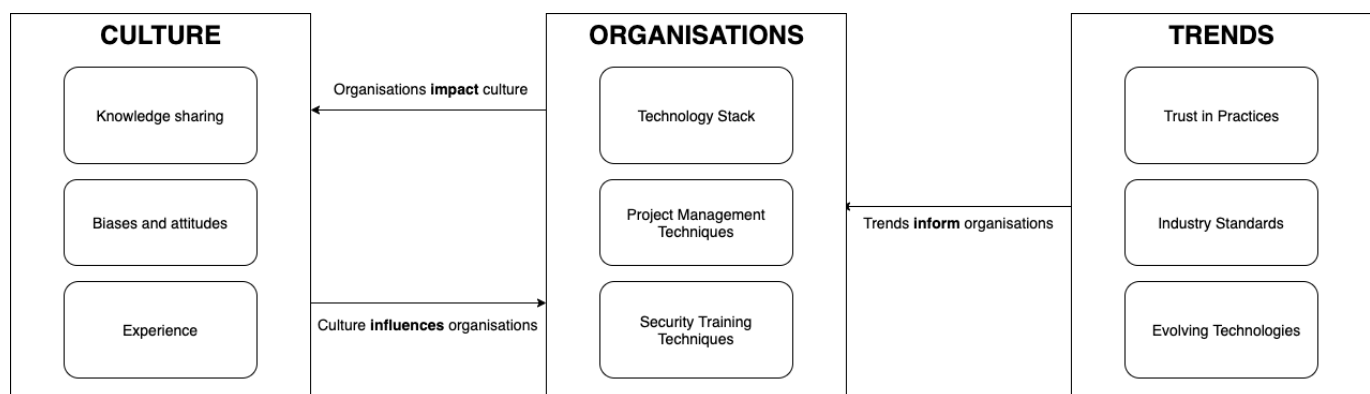
3. Industry trends

Figure 4.1: The diagram of the emergent Influences on Security Practices theory

A prior iteration of the diagram had shown one more category; "Teams". However, as the constant comparison process occurred, the factors of teams seemed to be more-so attributed to organisational structuring and practices. This meant that this category title was discarded and the factors were merged into "Organisations". Another discarded category was the influence of stakeholders. At the beginning of the interview process, clients and vendors seemed to have significant influence to the security practices implemented by programmers, but as the analysis process developed, it was not as strongly quoted in the data

collection. Even when prompted, the idea seemed to be foreign to many. Participants were disclosing that decisions were not dependent on any stakeholders and that set practices were already stipulated.

## 4.1 Culture

This category is a combination of the culture we see in groups of individuals. Important concepts relating to this were mentioned by the participants and were discovered in the data analysis. The term culture refers to the customs that programmers have in order to maintain security; knowledge sharing, biases and attitudes and experience.

### 4.1.1 Knowledge Sharing

Knowledge sharing was highly regarded among the participants. Participants identified communication between team-mates as being a key way to learn and better current and new security practices. These opportunities are done within teams and are often done when peer-programming or simply asking questions. However, often the vital knowledge sharing moments happened in passing. When programmers were stuck with using a library, framework or even learning a newer language nuance, they appreciated the ability to turn to the person next to them and get help. P10 identified this as:

**"INSERT QUOTE"**

The lack of knowledge sharing was often highlighted as a deterrence in learning and using practices. P11, described this as *"bro-culture"* where there is a view that asking questions make you seem lesser than, and therefore, there was a cultivated culture on this lack-of-communication.

P8 defined that the open communication streams between people across business and experiences made it easier to obtain answers. Walking between desks to other teams and also sending anyone emails no-matter the hierarchical nature of jobs titles helped facilitate these exchanges. These were often more attainable in smaller organisations where individuals were more familiar with each other **INSERT QUOTE YOU HAVE THIS SOMEWHERE - CHECK P5, P8, P9**.

### 4.1.2 Biases and attitudes: TODO

Participants had very strong preferences to how security practices aligned with their work. Those were strictly developers typically found it a deterrence in completing their work

### 4.1.3 Experience: TODO

Experience pertains to the level of expertise an individual has in the industry. This was not only measured by the amount of years that they have worked, but also whether they have worked on a range of projects. P11 is an example of this; they have worked 2-5 years in industry, but have worked in multiple government and private organisations in their short-time in the workforce. Their experiences are related to their background in the industry.
- Speed in picking up new tools - Identifying issues

## 4.2 Organisational

This category is the influence of organisational practices and structuring on security practices. The attributes within this category are the parts of an organisation which motivated programmer choices; technology stack, project management techniques and security training techniques.

### 4.2.1 Technology Stack

- organisations have already decided upon languages and frameworks and libraries
- languages don't often change because of security needs; quote both cloud engineers as outliers

### 4.2.2 Project Management Techniques

- devops vs agile vs waterfall
- promote talking between teams

### 4.2.3 Security Training Techniques

- still often quite traditional in just being more policy and protocol related.
- technical training is up to the person to do in their own personal training time at work - usually linkedin videos, pluralsite
- 3 outliers; p10 mentioned technical workshops in the form of a follow through tutorial sort of like pondy's live coding explanations in comp102, p13 and p14 mentioned corporate hackathons as a great way to learn and they really advocated for this

## 4.3 Trends

This category is the influence of industry trends on a programmer. The attributes within this category are the functions which make this category and impact the security related decisions which programmers make; trust in practices; industry standard, evolving technologies.

### 4.3.1 Trust in Practices

- open source libraries and frameworks. Most say they prefer enterprise, but even when they use open-source not a lot of testing goes on based on trust. outlier is P14 who is the only programmer to say that before they take upon new open-source tools they look at commit checking and document checking.
- gov organisations trust in vendor

### 4.3.2 Industry Standard

- compliance, laws,
- based on what industry is doing in a rush to match competitors

### 4.3.3 Evolving Technologies

- new uptake of cloud products (gov - P1 said i should focus on this), automation (P15 implements automation to existing services)

## 4.4 Connections between Categories

### 4.4.1 Trends Inform Organisations

### 4.4.2 Organisations Impact Culture

### 4.4.3 Culture influences Organisations

# Chapter 5

# Evaluation

- evaluate against methodology - evaluate the process

# Chapter 6

# Conclusions

## 6.1  Limitations

- Gender disbalance

- Really wide scope –¿ stuck to one role/one sector/similar years of experience

- Nature of the subject meant that NDA's were an issue when collecting data

## 6.2  Future Work

- Would be interesting to focus on organisational differences

- refine this to focus on one lot of people to get a more technical-based theory –¿ define technical sis

- study of the impacts of internal hackathons on less experienced people in industry

- a more robust educational programme in workplaces

## 6.3  Conclusion

# Bibliography

[1] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," *Software: Practice and Experience*, vol. 50, no. 3, pp. 275–298, 2020.

[2] M. of Health, "Cyber security incident." [Online]. Available: `https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident`, [Accessed May 31 2020].

[3] M. of Health, "Update on tū ora cyber security incident at 8 october 2019." [Online]. Available: `https://www.health.govt.nz/system/files/documents/pages/health_report_8_october_20191935_redacted.pdf`, [Accessed May 31 2020].

[4] M. John, F. Maurer, and B. Tessem, "Human and social factors of software engineering: Workshop summary," *ACM SIGSOFT Software Engineering Notes*, vol. 30, pp. 1–6, 07 2005.

[5] R. Hoda, J. Noble, and S. Marshall, "grounded theory for geeks," in *ACM International Conference Proceeding Series*, 2011.

[6] H. Assal and S. Chiasson, "think secure from the beginning," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI 19*, ACM Press, 2019.

[7] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security apis," *IEEE Security Privacy*, vol. 14, no. 5, pp. 40–46, 2016.

[8] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," *Software: Practice and Experience*, vol. 50, no. 3, pp. 275–298, 2020.

[9] S. G. Lorrie Faith Cranor, *Security and Usability*. O'Reilly Media, 2005.

[10] B. Julian, J. Noble, and C. Anslow, "Agile practices in practice: Towards a theory of agile adoption and process evolution," pp. 3–18, 04 2019.

[11] N. Newton, C. Anslow, and A. Drechsler, *INFORMATION SECURITY IN AGILE SOFTWARE DEVELOPMENT PROJECTS: A CRITICAL SUCCESS FACTOR PERSPECTIVE*, pp. 8–14. 06 2019.

[12] I. Facebook, "A tool to detect bugs in java and c/c++/objective-c code before it ships." [Online]. Available: `https://fbinfer.com/`, [Accessed May 31 2020].

[13] C. Sadowski, J. van Gogh, C. Jaspan, E. Soederberg, and C. Winter, "Tricorder: Building a program analysis ecosystem," in *International Conference on Software Engineering (ICSE)*, 2015.

[14] I. Synopsys, "Coverity scan static analysis." [Online]. Available: `https://scan.coverity.com/`, [Accessed May 31 2020].

[15] Raygun, "Raygun." [Online]. Available: `https://raygun.com/`, [Accessed May 31 2020].

[16] A. I. Security, "Cyber security market research report." [Online]. Available: `https://www.kordia.co.nz/aura-cyber-security-market-research-2019`, [Accessed May 25 2020].

[17] D. of the Prime Minister and Cabinet, "New zealand's cyber security strategy 2019." [Online]. Available: `https://dpmc.govt.nz/sites/default/files/2019-07/Cyber\%20Security\%20Strategy.pdf`, [Accessed May 25 2020].

[18] OWASP, "Owasp secure coding practices." [Online]. Available: `https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf`, [Accessed May 25 2020].

[19] D. Kirk and E. Tempero, "Software development practices in new zealand," in *2012 19th Asia-Pacific Software Engineering Conference*, vol. 1, pp. 386–395, 2012.

[20] C. Weir, J. Noble, and A. Rashid, "Challenging software developers: Dialectic as a foundation for security assurance techniques," Apr. 2020.

[21] SPG, "Alumni." [Online]. Available: `https://ecs.wgtn.ac.nz/Groups/SPG/Alumni`, [Accessed May 31 2020].

[22] L. Sajwan, "Why do programmers do what they do? recruitment webpage." [Online]. Available: `https://homepages.ecs.vuw.ac.nz/~sajwanlava/`, 2020.

# Appendix A

# Application

**ResearchMaster**

**Human Ethics Application**

| | |
|---|---|
| Application ID : | 0000028506 |
| Application Title : | Why Do Programmers Do What They Do? |
| Date of Submission : | 28/05/2020 |
| Primary Investigator : | Lavanya Sajwan; Principal Investigator |
| Other Personnel : | Prof James Noble; Supervisor |
| | Dr Craig Anslow; Associate Investigator |

**Research Form**

**Application Type**

Is this application for:*

◉ Research  ○ Teaching only

> Please select **'Research'** below and then select **'Save'** to access the rest of the form.

*

| Research |
|---|

## Research Overview

**Application Details**

1. Application ID

| 0000028506 |
|---|

2. Title of project
*(Click the ? icon for more info)**

| Why Do Programmers Do What They Do? |
|---|

3. School or research centre*

| Engineering and Computer Science |
|---|

4. The following questions will help the committee assess whether your application is categorised as a Category A (more than low risk) or Category B (low risk).

Please check all of the boxes that apply. You will be asked for more information about some of these questions later in the application.

Check the box if your study:

4a Is health research*
○ Yes ◉ No

4b Is an intervention study*
○ Yes ◉ No

4c Involves the use, collection or storage of human tissue*
○ Yes ◉ No

4d Involves processes that use EEG, ECG, MRI, TMS, FMRI, EMG, radiation, invasive or surface recordings*
○ Yes ◉ No

4e Involves collection of information about illegal behaviour, or information that has been obtained illegally*
○ Yes ◉ No

4f Involves people who are not giving consent to be part of the study (other than observational research in a public place)*
○ Yes ◉ No

4g Involves participants under the age of 16*
○ Yes ◉ No

4g (i) Will a parent/guardian be asked to give consent for the child/young person to participate in research?*
○ Yes ○ No ◉ N/A

4g (ii) Will more than one meeting be held with the child/young people without others present? *
○ Yes ○ No ◉ N/A

4h Involves participants whose ability to consent freely is compromised due to context (e.g. people in prison), or a limited capability to make independent rational decisions (e.g. those with a serious intellectual disability).*
○ Yes ◉ No

4i Involves the use of concealment or covert observations, including those conducted online or conducted in social media. *
○ Yes ● No

4j Involves the use of previously collected personal information, other data, or biological samples for the collection of which there was no explicit consent for use in research.*
○ Yes ● No

4k Involves deception of the participants, including concealment of the true purpose of the research*
○ Yes ● No

4l Involves the use of highly sensitive information (see policy for definition)*
○ Yes ● No

4m Involves a focus on, has particular importance for, or impacts on Māori*
○ Yes ● No

4n Involves any other group (for example cultural or religious), other than Māori, and has the potential to cause discomfort or disruption to members of that group*
○ Yes ● No

4o Involves any direct financial interest in the outcome of the research by any member of the research team or external sponsor*
○ Yes ● No

4p Involve a conflict of interest or the appearance of a conflict of interest for the researcher (for example, where the researcher is also the lecturer/teacher/treatment provider/colleague/manager or employer of the participants)*
○ Yes ● No

4q Involve any situation which may put the researcher at risk of harm (e.g. overseas in politically unstable countries)*
○ Yes ● No

4r Involve a reasonable expectation that participants may experience (at a greater level than in everyday life) physical discomfort, emotional discomfort, or psychological or spiritual harm (e.g. asking participants to recall upsetting events)*
○ Yes ● No


**Relationship to other Projects**

5. Does this application relate to any previous applications submitted to an ethics committee (at VUW or other Institute)?*
● Yes
○ No

5a. If this was a Victoria University of Wellington human ethics applications, please search and add the related ethics applications from the below search window.

**Search by title (partial or complete) or application ID (partial or complete):**

*This question is not answered.*

5a (i). If you can't find the application above, please enter the application number here.

| 0000024839 |
|---|

5a (ii). If this was an ethics committee from another institution, please upload supporting documentation (such as a letter of approval) in the document section.

5a (iii). If your research has been assessed by a Health and Disability Ethics Committee (HDEC) and found to be Out of Scope, please upload a copy of the Scope of Review form submitted to HDEC and the Out of Scope letter on the Documents page.


**Personnel**

Personnel
To add other researchers, enter their user name, if known, or search for their first or last name (whichever is the most unusual). Click the search icon to run the search, and select the person from the list view. Click on **'OK'** at the bottom right corner to save the person record.

| 1 | First Name | Lavanya |
|---|---|---|
| | Last Name | Sajwan |
| | Full Name | Lavanya Sajwan |
| | AOU system code | Engineering and Computer Science |
| | Position | Principal Investigator |
| | Primary Investigator? | Yes |
| 2 | First Name | Craig |
| | Last Name | Anslow |
| | Full Name | Dr Craig Anslow |
| | AOU system code | Engineering and Computer Science |
| | Position | Associate Investigator |
| | Primary Investigator? | No |

6. Are any of the researchers from outside Victoria?*

○ Yes
◉ No

7. Is the principal investigator a student?*

◉ Yes
○ No

**Student Researcher**

7a. What is your course code (e.g. ANTH 690)?*

ENGR489

7b. Supervisor

To add your supervisor enter their user name, if known, or search for their first or last name (whichever is the most unusual). Click the search icon to run the search, and select the person from the list view. Click on **'OK'** at the bottom right corner to save the person record. *

| 1 | Given Name | James |
|---|---|---|
| | Surname | Noble |
| | Full Name | Prof James Noble |
| | AOU | Engineering and Computer Science |
| | Position | Supervisor |

7c. What is your email address? (this is needed in case the committee needs to contact you about this application)*

sajwanlava@myvuw.ac.nz

**Scope of Research**

**Project Details**

8. Describe the aims and objectives of this project
Provide a brief summary in plain language of the purpose, research questions/hypothesis, and objectives of your project. *

This project will investigate how software programmers implement and adopt security practices in the work they do, in order to develop an understanding of the influences and impacts on decisions surrounding their technical work. Examples of influences can include: type of education, whether the organisation further educates the employees, and what programming languages have they had experiences with.

This project will be done by using grounded theory and interviews will to take place to collect the data, to which then analysis of answers will then need to occur.

9. Describe the benefits and scholarly value of the project
Briefly place the project in perspective, explaining its significance and worthwhile outcomes. Include how this project will build on relevant literature, including references if appropriate.
*

Qualitative research is often neglected and overlooked in favour of more quantitative reasoning and technical traits; the processing speed, the programmers task-completion rate. Programmers provide a human aspect to a technical solution and therefore, there should be a shift to understanding the more background 'soft' processes that occur when making decisions; why are the choices made based on past influences, and how they affect the programmers work in the present?

Exploring this topic is essential as it allows for more understanding on how and why programmers think the way they do, and it builds a more robust understanding of the human and social aspects of Software Engineering The findings of this can be used to identify what security methods developers find as beneficial in their programming. This will allow programmers to complete their work to a higher standard, thus overall making their work of a higher value.

10. Explain any ethical issues your research raises for participants, yourself as the researcher, or wider communities and institutions, and how you will address these. This is an opportunity to present what you think the key risks are in your project and show how you have taken them into account.*

The project aims to investigate how security practices are implemented and adopted in the work programmers in industry work on. Steps will need to be taken to ensure that the interview questions will be written in a way that does not reveal the individuals personal passwords or suggest any hints to it. As they will be professionals, the questions will also have to be worded in a way that does not expose specific business secrets. By doing both of these, the privacy of the person and the company can be maintained and protected. Participants will not require approval from organisations to partake in this study, as the participants will not be named in any produced texts, and therefore, will not be linked to any specific organisation. It will be explained to participants that they should not reveal any business secrets or passwords at the start of the interview, and this piece of information will also be stated in the supporting participant information sheet document.

There is also a risk of discovering an organisation's security practices, which means the interview data needs to be kept secure and confidential. For instance, any reports or publications should avoid including compromising information and allow interviewees to see their transcripts to comment and edit any information.

**Key Dates**

If approved, this application will cover this research project from the date of approval for up to 3 years.

11. Proposed start date for data collection*

06/07/2020

12. Proposed end date for data collection*

28/02/2021

13. Proposed end date for research project*

28/02/2021

**Proposed source of funding and other ethical considerations**

14. Indicate any sources of funding

- Internally: by a University grant, such as the University Research Fund
- Externally: funding from an external organisation for this project, or a scholarship awarded by an external organisation
- Self-funded: paying for research costs such as travel, postage etc. from your own funds

Tick all that apply:

☑ Internally funded

☐ Externally funded

☑ Self-funded

15. Is any professional code of ethics to be followed?*

○ Yes

◉ No

16. Do you require ethical approval from any other organisation, such as another tertiary institution in New Zealand or overseas, or a District Health Board?*

○ Yes

◉ No

**Data Collection and Recruitment**

**Data Collection**

17. Please select all forms of data collection you will use in your project*

30

☑ Interviews
☐ Focus groups
☐ Questionnaires
☐ Observation
☐ Other

18. Provide an explanation of the sampling rationale for your study.
E.g. representative sampling of a particular population, purposive sampling, convenience sampling. Include here your eligibility criteria for potential participants -- will there be particular criteria for participants to be included in your study, or criteria that will exclude them? *

> The study will follow purposeful sampling as the participants will be those working in the industry and ideally have a range of job titles associated with programming and years in the field in order to find interesting comparisons during the interview process in the way security practices are adopted in the developed software. They can be a part of any type of organisation; government, private, non-profit etc.
>
> Examples of appropriate jobs associated with the individuals can be; devops engineers, front-end security developers, database administrators, security architects etc.
>
> Participants will consequently be filtered by appropriate job titles and anyone younger than the age of 18.

19. How many participants will be involved in your research?
Please specify how many groups and how many participants in each group. *

> Up to 30 participants from the industry who are familiar with security practices through the professional work they do.

20. What are the characteristics of the people you will be recruiting?*

> The key characteristic of the individuals will be their programming experience, security education, and age. They will have a technical role within the organisation. The study hopes to capture a range of ages and levels experience in their role in order for in-depth comparisons for analysis. Therefore, there is no specific minimum or limit on the years of programming experience, or what kind of experience, and security education sought. However, participants do have to be at least 18 years old. Participants jobs will all be New Zealand based. Participants can also work across a range programming fields eg. gaming, education, financial, analysis.

21. Outline in detail the method(s) of recruitment you will use for participants in your study. Include here how potential participants will be identified, who will contact them and how. Please include copies of all advertisements, online posts or recruitment emails in the 'Documents' section. *

> I will make contact with sample groups with a request of participation by posting on groups, mailing lists and by using supervisor and my own connections. Such groups could be security groups on the websites, Meetup and Linkedin. Mailing lists can consequently be obtained from those groups as well.
>
> A pilot study will be conducted with 2-3 participants. These participants will be recruited directly by me and are all personal contacts; friends, and family friends.

22. Explain the details of the method of data collection. For example, describe the location of your research procedures, if appropriate (e.g. where your interviews will take place). If necessary, upload a research protocol in the 'Documents' section.*

> The interviews will be confidential rather than anonymous as they are done in-person and to also allow for follow up questions if necessary. Participants will be welcome to leave at any time during the interview, do not have to answer any questions they do not want to and can choose to leave the study within a week after the interview if they would like.
>
> Interviews should be done in safe and private environments, with all participants clear on earthquake and fire evacuation procedures relevant to their location. Due to the recent COVID-19 outbreak, I will offer zoom interviews for those who are unable or unwilling to meet directly. Consent can be obtained over email by sending the information sheet and consent form content to the participant in an email body and they reply to that email with "I consent".
>
> For in-person interviews, I will provide a box of tissues, a bottle of sanitiser, and maintain social distancing. The small meeting room will be wiped down and disinfected between interviews.
>
> The interviews will be voice recorded, and will then be transcribed.

23. Will your research project take place overseas?*
○ Yes
◉ No

24. Does the research involve any other situation which may put the researcher at risk of harm (e.g. gathering data in private homes)?*
○ Yes
◉ No

**Participants and Informed Consent**

25. Does your research target members of a vulnerable population?
This includes, but is not limited to, children under the age of 16, people with significant mental illness, people with serious intellectual disability, prisoners, employees and students of a researcher, and people whose health, employment, citizenship or housing status is compromised. Vulnerability is a broad category and encompasses people who may lack the ability to consent freely or may be particularly susceptible to harm.*
○ Yes
◉ No

26. Have you undertaken any consultation with the groups from which you will be recruiting, regarding your method of recruitment, data collection, or your project more widely?*

○ Yes
◉ No

27. Will your participants receive any gifts/koha in return for participating?*

◉ Yes
○ No

27a. Describe the gifts/koha and the rationale.*

All individuals who participated in the interviews will be given a $10 supermarket voucher, and all will go into the draw to win a $60 supermarket voucher to thank them for their time and provide them with an incentive.

28. Will your participants receive any compensation for participation (for instance, meals, transport, or reimbursement of expenses)?*

○ Yes
◉ No

29. How will informed consent be obtained? (tick all that apply to the research you are describing in this application)*

☐ Informed consent will be implied through voluntary participation (anonymous research only)
☐ Informed consent will be obtained through a signed consent form
☑ Informed consent will be obtained by some other method

29a. Describe the other method*

Participants can consent over email by simply sending the consent form content to the participant in an email body and they reply to that email with "I consent".

## Treaty of Waitangi

### Treaty of Waitangi

30. How does your research conform to the University's Treaty of Waitangi Statute? (you can access the statute from Victoria's Treaty of Waitangi page)*

The study does not involve knowledge directly related to Te Āo Māori but care should be taken to encourage the participation of Māori under the principle of Whai wāhi (participation). To encourage this, the study will be advertised to organisations where there is more emphasis on using Te Tiriti o Waitangi as part of their core values.

## Project Risks

### Minimisation of Harm

31. Is it possible that participants may experience any physical discomfort as a result of the research?*

○ Yes
◉ No

32. Is it possible that participants may experience any emotional or psychological discomfort as a result of the research? (E.g. asking participants to recall upsetting events, viewing disturbing imagery.)*

○ Yes
◉ No

33. Will your participants experience any deception as a result of the research?*

○ Yes
◉ No

34. Is any third party likely to experience any special hazard/risk including breach of privacy or release of commercially sensitive information? This may occur in the instance participants are asked to discuss identifiable third parties in the research.*

◉ Yes
○ No

34a. Give details and indicate how you will manage this*

As this study involves questioning individuals on the security practices they implement in the software they develop there is a risk of exposing the company they work for. However, as outlined in question 10 of this application, there will be steps to prevent this happening by being careful of how questions are phrased. These include not publishing the interviewee and corresponding organisation name in any texts that are the result of this research.

35. Do you have any professional, personal, or financial relationship with prospective research participants? *

○ Yes
◉ No

36. What opportunity will participants have to review the information they provide? (tick all that apply)*

☐ Will be given a full transcript of their interview and given an opportunity to provide comments
☐ Will be given a full transcript of their interview and NOT given an opportunity to provide comments
☐ Will be given a summary of their interview
☑ Other opportunity
☐ Will not have an opportunity to review the information they provide

36a. Please give details*

Participants can be given a recording of their interview and have the opportunity to add/edit/remove details up to 1 week after the interview has taken place.

**Confidentiality and Anonymity**

37. Will participation in the research be anonymous?
**'Anonymous'** means that the identity of the research participant is not known to anyone involved in the research, including researchers themselves. It is not possible for the researchers to identify whether the person took part in the research, or to subsequently identify people who took part (e.g., by recognising them in different settings by their appearance, or being able to identify them retrospectively by their appearance, or because of the distinctiveness of the information they were asked to provide).*

○ Yes
◉ No

38. Will participation in the research be confidential?
**'Confidential'** means that those involved in the research are able to identify the participants but will not reveal their identity to anyone outside the research team. Researchers will also take reasonable precautions to ensure that participants' identities cannot be linked to their responses in the future.*

◉ Yes
○ No

38a. How will confidentiality be maintained in terms of access to the identifiable research data? (tick all that apply)*

☐ Access to the research will be restricted to the investigator
☑ Access to the research will be restricted to the investigator and their supervisor
☐ Focus groups will have confidentiality ground rules
☐ Transcribers will sign confidentiality forms
☐ Other

38b. How will confidentiality be maintained in terms of reporting of the data? (tick all that apply)*

☑ Pseudonyms will be used
☑ Data will be aggregated
☑ Participants will be referred to by role rather than by name
☐ Other

38b (i). Please provide details*

Participants in the study will not be named in any reports or summaries produced. The study uses grounded theory methodology so the people and the answers will be grouped to form a final theory on what influences programmers to make the decisions they do. The purpose of the study is not to focus on the individuals, but rather draw conclusions and similarities from their responses. Instead, the study will likely compare different groups of people based on key variables such as computing experience. Participants will not be directly quoted, and will be referred to by role or pseudonyms.

39. Will participation in the research be neither confidential nor anonymous, and participants will be identifiable in any outputs or publications relating to the research? *

○ Yes
◉ No

**Data Management**

**Access, Storage, Use, and Disposal of Data**

40. Which of the following best describes the form in which data generated in your study will be stored during the study?
See help text for guidance on these terms. Further info available on human ethics website.*

○ Identifiable
○ Potentially identifiable
● Partially de-identified
○ De-identified
○ Anonymous
○ Other

41. Which of the following best describes the form in which data generated in your study will be stored after the study is completed?
See help text for guidance on these terms. Further info available on human ethics website.*
○ Identifiable
○ Potentially identifiable
○ Partially de-identified
● De-identified
○ Anonymous
○ Other

42. Proposed date for destruction of identifiable research data (i.e. the date when data will be de-identified and personal information on participants destroyed)

*

| 31/12/2021 |

43. Proposed date for destruction of de-identified research data, including anonymous data

*

| 31/12/2021 |

44. Will any research data be kept for longer than 5 years after the conclusion of the research?*
○ Yes
● No

45. Who will have access to identifiable, de-identified or anonymous data, both during and at the conclusion of the research?*
○ Access restricted to the researcher only (whoever is named as PI)
● Access restricted to researcher and their supervisor
○ Access restricted to researcher and immediate research team, e.g. co-investigators, assistants
○ Other

46. Are there any plans to re-use either identifiable, de-identified or anonymous data?*
○ Yes
● No

47. What procedures will be in place for the storage of, access to and disposal of data, both during and at the conclusion of the research? (Check all that apply)
Information regarding appropriate data storage is available on the human ethics website. Note that storing research data on USB drives is strongly discouraged for security reasons. *
☑ All hard copy material will be stored securely e.g. in a locked filing cabinet
☑ All electronic material will be held securely, e.g. only on University servers, password protected
☑ All hard copy material will be appropriately destroyed (e.g. shredded) on the dates given above
☑ All electronic data will be deleted on the dates given (ITS should be consulted on proper method)

**Dissemination**

**Dissemination**

48. How will you provide feedback to participants?*
| I will offer participants the opportunity to request for a copy of their interview recording. |

49. How will results be reported and published? Indicate which of the following are appropriate. The proposed form of publications should be indicated to participants on the information sheet and/or consent form*
☑ Publication in academic or professional journals
☑ Dissemination at academic or professional conferences
☑ Availability of the research paper or thesis in the University Library and Institutional Repository
☐ Other

50. Is it likely that this research will generate commercialisable intellectual property?
*(Click the ? icon for more info)*

○ Yes
◉ No

**Supporting Documents**

**Documents**

51. Please upload any documents relating to this application. Sample documents are available on the [Human Ethics web page](#).

- Ensure that your files are small enough to upload easily, and in formats which reviewers can easily download and review.
- To upload a document click on the green arrow to the right of the named document. Follow the on screen instructions which will be displayed to upload a document.
- To replace a document, click the tick in the column to the right of the document you want to replace, and follow the screen instructions to continue.
- To add a new document click on 'New Document', at top right of the documents table. You **must** enter the document name in the box that appears. Click on 'OK'. Click on the green arrow which appears to the right of the file name to continue.
- Collate all your documents into one PDF or Word file, and upload as a new document. This should be labelled as 'Combined Documents'.

*

| Description | Reference | Soft copy | Hard copy |
|---|---|---|---|
| Participant information sheet(s) | Participant_Information_Sheet.pdf | ✓ | |
| Participant consent form(s) | Consent_to_Interview.pdf | ✓ | |
| Interview questions or guide | Interview_Guide.pdf | ✓ | |
| Application Changes | Changes_Summary.docx | ✓ | |
| Recruitment Posts | Recruitment_Post.pdf | ✓ | |

**Application Sign Off**

**Application Feedback**

**Feedback**

This page will be used to provide feedback between the Research Office and the researcher/s during the application review process.

## Committee response to your application

**Date**

15/05/2020

Comments

Hi,
Please refer doc attached.
Thanks

Documents

28506_Sajwan_Revise and Resubmit.docx

**Researcher response to requirements: please enter your comments below and then save.**

*This question is not answered.*

If you have been asked to provide a response to the committee's comments in a document, please upload that document here and then **save**.

Changes_Summary.docx

## Further required changes

**Date**

*This question is not answered.*

Comments

*This question is not answered.*

Documents

*This question is not answered.*

**Researcher response to requirements: please enter your comments below and then save.**

*This question is not answered.*

If you have been requested to respond to further feedback by uploading documentation here, please upload and then **save**.

*This question is not answered.*

**Final Review Outcome**

Final Review Outcome

*This question is not answered.*

Formal Notice of Approval

*This question is not answered.*

**Risk Category**

Based on answers to the screening questions (Q4), your application will be assessed as either Category A (higher than low risk), or Category B (low risk). The risk category will be reviewed by the Research Office before it is processed by the committee.

The risk assessment for this application is currently:

**Category B (LOW RISK)**

**Incident Report (admin only)**

**Incident Reporting**

## Incident Report

**Adverse incidents are instances of potential or actual physical harm to participants or researchers; emotional harm or distress to participants or researchers; and any other unforeseen events that raise ethical issues.**

Research teams must immediately advise the Human Ethics Committee if an adverse incident occurs in the course of their research project.

An incident report form can be obtained by sending an email to Ethics Administrator

The full incident report should be returned by email, and the committee administrator will upload it to this application

**For Admin Use**

Is there an incident to report?

☐ Yes
*This question is not answered.*

Do you have a second incident to report?
☐ Yes
*This question is not answered.*

37

# Appendix B

# Participant Information Sheet



## *Why do Programmers Do What They Do?*

### INFORMATION SHEET FOR PARTICIPANTS

You are invited to take part in this research. Please read this information before deciding whether or not to take part. If you decide to participate, thank you. If you decide not to participate, thank you for considering this request.

### Who am I?

Kia ora koutou! My name is Lavanya Sajwan and I am an Honours student in the school of engineering and computer science at Victoria University of Wellington. This research project is work towards partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering.

### What is the aim of the project?

This project is an informative investigation on how software programmers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impact decisions surrounding their technical work. Your participation will support this research by providing insight to the solutions that programmers are using to implement in their security practices. Essentially this research aims to gather your experiences and compare them with those of your peers to understand the use of security practices in the New Zealand industry. This research has been approved by the Victoria University of Wellington Human Ethics Committee (Research Master Application ID: 0000028506).

### How can you help?

You have been invited to participate because you are a professional programmer in the industry, familiar with working with security practices, and are over the age of 18 and this project aims to develop a theory as to why programmers implement and adopt security practices in the work, they do by interviewing professional programmer. It is important to gather data from individuals with varying career timelines and progressions as the data can be thoroughly analysed to form connections. I will interview you at Victoria University of Wellington's Kelburn campus, via Zoom or at another venue of your choice. I will ask you questions about your security practices and habits in your day-to-day work and how you make decisions regarding your methods of choice. It is advised that you refrain from naming any 3rd parties. If you agree to take part the interview will take 30-60 minutes of your time. I will audio record the interview with your permission and write it up later. You can choose to not answer

any question or stop the interview at any time, without giving a reason. You can withdraw from the study up to 1 week after the interview has taken place. If you withdraw, the information you provided will be destroyed. You may also choose to receive a copy of the interview recording which will be emailed to you, and you will have the opportunity to edit, appended and remove details up to 1 week after receiving the recording. You will be given a $10 supermarket voucher and go into the draw for a $60 supermarket voucher as koha to thank you for your time.

## What will happen to the information you give?

This research is confidential, but may be limited due to small sample and nature of the research. You and your organisation will not be named in the final report, but title may be named and persons within or familiar with your organisation and title may be able to identify you and your organisation based on the distinctiveness of the information you provide. However, you may choose to not have any potential identifying information published.

Please do not name any 3<sup>rd</sup> parties and reveal any business secrets and passwords.

Your name and email address will be used to contact you in the event of winning the overall prize, and when a recording of your interview is sent if you choose to receive it.

Only my supervisors and I will read the notes of the interview. The interview summaries and any recordings will be kept securely and destroyed on the 31st of December 2021.

## What will the project produce?

The information from my research will be used in my Honours report and presentation. You will not be identified in either of these materials or in any supplementary reports such as publications in academic or professional journals.

## If you accept this invitation, what are your rights as a research participant?

You do not have to accept this invitation if you don't want to. If you do decide to participate, you have the right to:

• choose not to answer any question;
• ask for the recorder to be turned off at any time during the interview;
• withdraw from the study up to 1 week after the interview has taken place;
• ask any questions about the study at any time;
• receive a copy of your interview recording;
• edit/append/remove any details up to 1 week after the interview.
• be able to read any reports of this research by emailing the researcher to request a copy.

**If you have any questions or problems, who can you contact?**

If you have any questions, either now or in the future, please feel free to contact any of either one of the people listed:

**Student Researcher:**

Name: Lavanya Sajwan
University email address: sajwanlava@myvuw.ac.nz

**Primary supervisor:**

Name: James Noble
Role:  Professor of Computer Science, Associate Dean (Postgraduate Research)
School: Engineering and Computer Science, Victoria University of Wellington
Phone: 04 463 6736
kjx@ecs.vuw.ac.nz

**Secondary supervisor:**

Name: Craig Anslow
Role: Senior Lecturer
School: Engineering and Computer Science, Victoria University of Wellington
Phone: 04 463 6449
craig.anslow@ecs.vuw.ac.nz

**Human Ethics Committee information**

If you have any concerns about the ethical conduct of the research you may contact the Victoria University HEC Convenor: Dr Judith Loveridge. Email hec@vuw.ac.nz or telephone +64-4-463 6028.

# Appendix C

# Participant Consent Form

### Why do Programmers Do What They Do?

**CONSENT TO INTERVIEW**

This consent form will be held for 5 years.

Researcher: Lavanya Sajwan, School of Engineering and Computer Science, Victoria University of Wellington.

- I have read the Information Sheet and the project has been explained to me. My questions have been answered to my satisfaction. I understand that I can ask further questions at any time. The end research date is: 28th of February 2021.

- I agree to take part in an audio recorded interview.

I understand that:

- I may withdraw from this study up to 1 week after the interview has taken place and any information that I have provided will be destroyed.

- Any information gathered will be securely stored on an ECS lab machine and any information I have provided will be destroyed on the 31st of December 2021.

- I understand that the findings may be used for an Honours report and a summary of the results may be used in academic reports and/or presented in conferences.

- I understand that the any information I provide will be kept confidential to the researcher and the supervisors.

- My name and my organisation name will not be used in reports, but persons within or familiar with the organisation practices may be able to identify me based on distinctiveness of the information I provide.

- I have the right to edit/append/remove details up to 1 week after the interview.

- I would like a copy of the recording of my interview:                    Yes ☐   No ☐

- I would like to receive a copy of the final report and have added my email   Yes ☐   No ☐
  address below.

Signature of participant:          _____

Name of participant: _____

Date: _____

Contact details: _____

# Appendix D

# Interview Questions



*Why do Programmers Do What they Do? – Potential Interview Questions*

**Participant Background**

- How many years' experience do you have?
- What is your current role and what does this entail?
- Please describe any security education you had **before** working at your current job?
- Would you like to tell me anything more about your background or experience in the industry?

**Current Work**

- Can you give a brief overview of the security features (protocols, frameworks, libraries, tools) that you regularly use at work?
- Do you know those practices have been tested within your team/organisation?
- Do you change languages based on the security practice you use? Why?
- Please share if you and your team have adapted any of the approaches to suit your work better
- Does your work provide any training, or is it expected that you how to program "securely"?
- What are some difficulties in joining a team with an established process?
- How does security fit in the development life-cycle in real life?

**Impacts**

- How have your chosen practices affected your ability to deliver within constraints?
- Have you experienced any data/security breaches as a consequence of your work and how was it managed?
- Have there been any lessons learned in your own personal projects and style?

**Experience-Based (Dependent on role and years of experience)**

- What recommendations would you generally give to teams looking to adopt your security practice of choice?

- Do you give other teams/individuals feedback on their security practices?
- What differences do you see between new and experienced people?
- What common "mistakes" do you see?
- What factors contribute to a successful education on how to use security practices?
- What difficulties did the teams you have worked with share?
- What changes have you observed in the security programming landscape in New Zealand?
- What are the current motivators and deterrents to programmers in terms of paying attention to security?

- IF FROM OVERSEAS OR WORKED OVERSEAS, WHAT DIFFERENCES HAVE THEY NOTICED IN SECURITY IN WORKPLACES IN NZ COMPARED TO OVERSEAS.

Any other issues or comments?

# Appendix E

# Recruitment Post

**Groups/Mailing List Post:**

Kia ora koutou!

My name is Lavanya Sajwan and I am a Software Engineering student at Te Herenga Waka - Victoria University of Wellington. I am working on an honours project this year which is about security practices in industry and investigating the influences impacting the decisions of the choice that developers make. This research has been approved by the Victoria University of Wellington Human Ethics Committee (Research Master Application ID: 0000028506).

I am looking to interview professional programmers who work with security practices, and will need to be over 18 years old and New Zealand based. Participants can also work across a range programming fields eg. gaming, education, financial, analysis.

If this is you and are interested in participating in this study please send me an email stating your interest including name and job title.

If you participate in the interview, you will be given koha of a $10 voucher, and go into the draw to win a $60 supermarket voucher to thank you for your time!

If you are interested in participating or hearing more about the study please contact me over email – sajwanlava@myvuw.ac.nz

Ngā mihi

# Appendix F

# Recruitment Webpage

## Why Do Programmers Do What They Do?

VUW Honours Project 2020

Research Master Application ID: 0000028506

### Who Am I?

...

Kia ora koutou! My name is Lavanya Sajwan and I am an Honours student in the school of engineering and computer science at Victoria University of Wellington. This research project is work towards partial fulfilment of the requirements for Bachelor of Engineering with Honours in Software Engineering.

### What is the Aim of the Project?

...

This project is an informative investigation on how software developers implement and adopt security practices in the work they do in order to develop an understanding of what influences and impacts decisions surrounding their technical work. Your participation will support this research by providing insight to the solutions that developers are using to implement in their security practices. Essentially this research aims to gather your experiences and compare them with those of your peers to understand the use of security practices in the New Zealand industry.

### How Can You Help?

...

The process that I will be following is through using Grounded Theory as a framework. Therefore, I need to interview many participants in order to gain enough information to form a theory around my findings. Participants should be professional programmers in industry and are over the age of 18 whom implement and adopt security practices at work.

## Interested?

Get in contact with any of the people listed below

**Researcher**

Lavanya
Sajwan
sajwanlava@myvuw.ac.nz

**Supervisors**

James
Noble
kjc@ecs.vuw.ac.nz

Craig
Anslow
craig@ecs.vuw.ac.nz