TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Nadezda Semjonova – 192927IVSB

Guidelines for Developing Cyber Security Culture: the Case of Pipedrive OÜ

Bachelor's thesis

Supervisor: Jesse Wojtkowiak
(Master of Science,
Chief Information
Security at Pipedrive)

Co-Supervisor: Kieren Nicolas Lovell
(Head of TalTech
Computer Emergency
Response Team,
Head Information
Security at Pipedrive)

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Nadezda Semjonova – 192927IVSB

Juhised küberturvalisuse kultuuri arendamiseks Pipedrive OÜ näitel

Bakalaureusetöö

Juhendaja: Jesse Wojtkowiak
(Master of Science,
Chief Information
Security at Pipedrive)

Kaasjuhendaja: Kieren Nicolas Lovell
(Head of TalTech
Computer Emergency
Response Team,
Head Information
Security at Pipedrive)

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Nadezda Semjonova

16.05.2022

Abstract

There are currently a lack of general guidelines and knowledge for implementing Security Culture Framework in a way that optimizes its effectiveness. This thesis aims to fill that gap by providing guidelines and sample analysis for organizations and cyber security specialists.

Quantitative online surveys were conducted using a voluntarily response sampling method. This method was chosen because it collects data using predetermined classifications and categories and allows for specialized and targeted research. The Security Culture Diagnostic Survey adopted an ipsative scale to measure answers, with ten questions and four responses that were to be assigned a score of ten points, divided among the responses according on how strongly or weakly each statement represents the organization. A Likert scale with a range of responses ("Strongly Disagree" to "Strongly Agree") was utilized in the Security FORCE Survey that provides a series of answers that go from one extreme to another with less extreme choices in the middle.

Analysis of 289 responses of Security Culture Survey revealed that dominant security culture present is a Trust Security Culture. This indicates that employees see their environment as their own and invest most of themselves in teamwork and for the benefit of Pipedrive. People define security as a shared responsibility in which all members participate and collaborate as a team to ensure the success of the organization. People are seen as security advocates, not threat actors in a risk equation. Analysis also showed some immediate value discrepancies within different teams and that is an indication of competing cultures within the company.

Analysis of 372 responses of Security FORCE Survey revealed that Security Value of Operations and corresponding key value behaviours are in line with Highly Reliable Security Programs.

This thesis claims that using the framework and guidelines proposed by the author, such as evaluating exciting and competing security cultures, and conducting behavioural

assessment, organizations and security professionals can ensure themselves with a structural process of transformation towards the desired security culture.

This thesis is written in English and is 121 pages long, including 7 chapters, 31 figures, 5 tables.

Annotatsioon

Praegu puuduvad üldised juhised ja teadmised julgeolekukultuuri raamistiku rakendamiseks selle tõhusust optimeerival viisil. Selle lõputöö eesmärk on täita see lünk, pakkudes organisatsioonidele ja küberturvalisuse spetsialistidele juhiseid ja näidisanalüüsi.

Kvantitatiivsed veebiküsitlused viidi läbi vabatahtliku vastuse valimi meetodil. Seda meetodit kasutati, kuna see kasutab andmete kogumisel eelnevalt määratud klassifikatsioone ja kategooriaid ning pakub spetsiifilisi ja sihipäraseid uuringuid. Turvakultuuri diagnostikauuringus kasutati vastuste mõõtmiseks ipsatiivset skaalat, mis koosnes 10 küsimusest nelja vastusega, mis tuleb määrata 10 punktiga, jagades need vastuste vahel vastavalt sellele, kui tugevalt või nõrgalt iga väide organisatsiooni peegeldab. Turvalisuse FORCE uuringus kasutati Likerti skaalat erinevate vastustega ("Ei ole täiesti nõus" kuni "Nõustun täielikult"), mis annab rea vastuseid, mis lähevad ühest äärmusest teise, mille keskel on vähem äärmuslikud valikud.

Küberturvakultuuri uuringu 289 vastuse analüüs näitas, et valitsev turvakultuur on usalduse turvakultuur. See näitab, et töötajad näevad oma töökeskkonda enda omana ning panustavad suurema osa sellest meeskonnatöösse ja ka Pipedrive'i hüvedesse. Inimesed defineerivad turvalisust kui jagatud vastutust, milles kõik liikmed osalevad ja teevad meeskonnana koostööd, et tagada organisatsiooni edu. Inimesi nähakse riskivõrrandis turvalisuse eestkõnelejatena, mitte ohus osalejatena. Analüüs näitas ka mõningaid vahetuid väärtuste erinevusi eri meeskondade sees ja see viitab konkureerivatele kultuuridele ettevõtte sees.
FORCE küsimustiku analüüs millele vastas 372 inimest, näitas, et toimingute turvaväärtused ja vastavad võtmeväärtuse käitumised on kooskõlas väga usaldusväärsete turbeprogrammidega.
Antud lõputöö väidab, et kasutades autori pakutud raamistikku ja juhiseid, nagu põnevate ja konkureerivate turvakultuuride hindamine ning käitumise hindamise läbiviimine,

saavad organisatsioonid ja turvaspetsialistid tagada end struktuurse transformatsiooniprotsessiga soovitud turvakultuuri suunas.

See lõputöö on kirjutatud inglise keeles ja on 121 lehekülge pikk, sealhulgas 7 peatükki, 31 joonist, 5 tabelit.

List of abbreviations and terms

COVID-19	Coronavirus Disease 2019
CRM	Customer Relationship Management
CSC	Cyber Security Culture
CSCF	Competing Security Culture Framework
DoS	Denial of Service
ENISA	European Union Agency for Network and Information Security
FORCE	Failure, Operations, Resilience, Complexity, Expertise
HRO	Highly Reliable Security Organizations
HRSP	Highly Reliable Security Program
InfoSec	Information Security
IT	Information Technology
SAT	Security Awareness Training
SCDS	Security Culture Diagnostic Survey

Table of contents

List of figures

List of tables

1 Introduction

1.1 Thesis Motivation

Over the last two years there has been a huge demand in technological innovations and new digital solutions. Social networking, online schooling, remote works and Internet of Things has the potential to make our world more complex than it has ever been before. With the progress the technology has become cultural, and the culture also has become technological. Culture has long been associated with views, believes, customs and ideas of the people and it influence the way they live their lives. Security culture is a culture that influence organization's security, it encompasses social behaviors and includes additional knowledge of critical dimensions: behavior, communication, attitude, cognition, compliance, standards and responsibilities [1].

An increase in the frequency of security events from both internal and external threats can be caused by a weak or non-existent security culture. Conversely, a strong security culture that integrated into decision-making processes and day-to day thinking, can create an almost impenetrable shield and truly increase the level of security.

Regardless of the size of an organization or industry of the business, there is an opportunity to create a people-centric security culture, where everyone is working towards the same goals and moving in the same direction in terms of cybersecurity. In a strong security culture, everyone is aware of the risks and has the will to contribute to minimizing the danger through their actions.

The main purpose of this work is to demonstrate the importance of assessing and improving the organization's security culture. Humans must be seen not as threat actors, but as assets capable of solving many of today's security problems.

1.2 Problem Statement

In the presented thesis an overview of the problem that there is insufficient understanding of importance of security culture in the industries and therefore no holistic guidelines exist to evaluate the organization's security culture to reduce cyber threats.

The importance of developing an effective security culture that shared by everyone in an organization is undervalued and not very well researched. Therefore, careful consideration was made in choosing appropriate methodology for the research due to the importance for future development and the continued assessment.

This research will be a case study built and diagnosed based on the proposed framework of "People-Centric Security, Transforming Your Enterprise Security Culture", by Lance Hayden (PhD) [2]. This particular framework was chosen because it is backed by a tremendous amount of research and academic studies and can be applied in real-world scenarios.

The main goal of this thesis is application of an existing cyber security culture framework within the Pipedrive enterprise and to develop visibility into the desired security culture. Data from two surveys, as well as Security FORCE metrics, will be collected and evaluated in order to assess and identify the corresponding values that are most prevalent within the Highly Reliable Security Program [2].

To achieve this goal, the collected data will be analyzed, and a set of guidelines will be developed that will benefit industries, such as Pipedrive, with their security strategies and serve as a framework for strengthening their security culture.

The continued assessment will be made in the future to determine if implemented guidelines are being followed, and whether or not employees are embracing the security culture.

2 Theoretical Background

This chapter covers the basics of information security and user behavior, the impact of Security Culture on cyber security in various industries and organizations.

2.1 Cyber Security Culture Definition

For the purposes of this research study, the author chose the definition provided by ENISA and it defines as follows:
Cyber Security Culture (CSC) of organizations refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cyber security and how they manifest in people's behavior with information technologies. CSC is about making information security principles an integral part of an employees' job, behaviors and conduct, incorporating them in their day-to-day actions [3].

2.2 Available Research

Various research initiatives on the definition of information security culture have been done such as Martins & Eloff 2002, Nosworthy, 2000 [4], Kuusisto and Ivonen, 2003 [5], Da Veiga, 2008 [6], Van Niekerk and Von Solms, 2010 , Hayden Lance, 2016 [2], ENISA, 2017 [3]. Other research focused on principles, such as Zakaria & Gani 2003 [7], OECD 2005 [8] and frameworks by Dojkovski, 2007 [9], Van Niekerk and Von Solms, 2006 [10], Martins and Eloff, 2002 [11], Hyden Lance, 2015 [2]. Studies were also done on the evaluation of an information security culture by Martins & Eloff, 2002 [11], Schlienger & Teufel 2005 [12] and Lance Hayden, 2015 [2].

A summary of some of the available research can be seen below in the Table 1 developed by Adele Da Veiga [6].

Research perspective		Definition	Cultivate				Assess				Total number of ticks
			Principles	Framework	Organisational behaviour tiers	Culture levels	Assessment instrument (Questionnaire)	Assessment instrument			
								Content validity	Construct validity	Reliability	
1	Gaunt (2000)	-	-	-	-	-	-	-	-	-	0
2	Nosworthy (2000)	✓	✓	-	-	-	-	-	-	-	2
3	Information Security Forum (2000)	✓	✓	-	-	-	-	-	-	-	2
4	Martins and Eloff (2002)	✓	✓	✓	✓	-	✓	✓	-	-	6
5	Kuusisto, Ilvonen, Helokunnas and Kuusisto (2003)	✓	✓	-	-	-	✓	-	-	-	3
6	Zakaria and Gani (2003, 2006)	-	✓	-	-	✓	-	-	-	-	2
7	Schlienger and Teufel (2002, 2003, 2005)	✓	✓	-	✓	✓	✓	✓	✓	✓	8
8	OECD (2005)	-	✓	-	-	-	-	-	-	-	1
9	Tessem and Skaraas (2005)	-	✓	-	-	-	-	-	-	-	1
10	Dojkovski, Lichtenstein and Warren (2006)	-	✓	✓	-	-	-	-	-	-	2
11	Thomson, Von Solms and Louw (2006)	-	✓	-	-	✓	-	-	-	-	2
12	Kraemer and Carayon (2005, 2007)	-	✓	-	-	✓	-	-	-	-	2
13	Ruighaver, Maynard and Chang (2006)	-	✓	✓	-	✓	-	-	-	-	3
14	Van Niekerk and Von Solms (2005, 2006)	✓	✓	✓	-	✓	-	-	-	-	4

Table 1. Research perspectives on information security culture [6]

One of the most comprehensive works on security culture was developed by Professor Hayden Lance in his book People-Centric Security 2016, where he covers all aspects related to security culture.

2.3 The Current State of the Cyber Security

The last two years of Corona crises showed us how unprepared we are and uncovered the necessity of the rapid changes within organizations across all industries. According to CoveWare [13], 2020 saw ransomware payments reach an all-time high and the most common method used by attackers to gain access to the critical systems is by social engineering. Phishing attacks surpassed all other techniques used by hackers and expected to see even higher increase in coming years.

One important reason for the success of a phishing attack is that attacks are designed to exploit human cognitive biases instead of technological loopholes. Phishing criminals often masquerade as a credible figure and broadcast manipulative email messages, instant messages or short messages is a large population. While reality reports may not be difficult to refute with some research. At first glance, the victims are usually taken by surprise. Thus, phishing victimization bypasses technological controls by manipulating human tendencies and information treatment. Thus, psychological and behavioral factors perhaps play a more important role [14].

According to the research by Ponemon Institute (2013), a significant percentage of breaches were due to human factors (35%), followed by system glitches (29%) and malicious or criminal attacks (37%) [15] .

The establishment of a strong information security culture in the organization is a necessary for effective information security [16] [10]. By measuring and assessing employee's security culture, organizations can adjust their training programs and improve policies because security culture must be accompanied by proper information security awareness.

Based on Security Culture and Credential Sharing, 2021, Research [17] revealed that last year Education and Legal industries improved their security culture score. This improvement may be explained that education and legal processes being moved to virtual settings due to the Covid-19 pandemic and the associated training changes. Unfortunately, industries like Construction, Consumer and Business Services showed reduction in security culture score. This could be explained by the fact that the manpower was downsized during the crisis.

Based on the report [17] with increase of security culture score industries showed significant improvement in reduction of the security risks, for an example, Education industry reduced the risk of employees sharing credentials by three times.

2.4 Security Indicators

The more the employees are trained, the more they understand the risks that are inherent in using email, leaving their computer unlocked, using the same password and similar everyday work behavior. With COVID-19 pandemic a lot of employees transitioned from in-office workplace to an at-home work environment, therefore employers had to find the new ways to secure employee's activities and to provide updated security trainings. While understanding of cyber threats has improved in 2021, understanding of social engineering threats is still alarmingly very low.

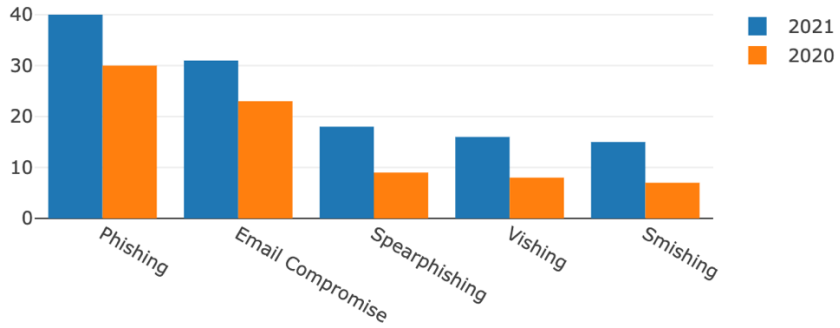

Figure 1. Percentage of employees who understand Social Engineering Threats "Very Well" [18]

Addressing key security issues and understanding of social engineering threats vary greatly from industry to industry.

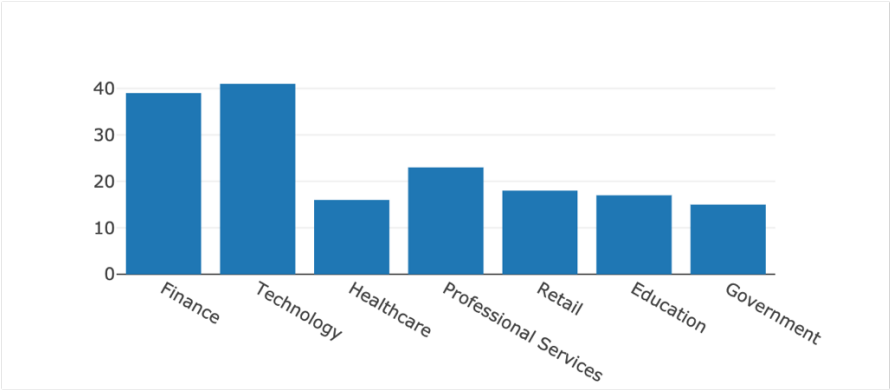

Figure 2. Extent to which employees in various industries understand Social Engineering threats [18]

The Impact of working from home carried with significant increases in ransomware, phishing and other malicious activities. Unfortunately, many employees lack the confidence in understanding important cybersecurity concepts and unable to identify key attack vectors and detect malware infection.

Issue	*Very Confident*	*Confident*	*Not Sure*	*Somewhat Confident*	*No Confidence*
You can identify a phishing email	42	34	10	10	4
Your current set of passwords are strong and have not been previously compromised	42	35	11	8	3
You can confidently describe the steps needed to work remotely securely	31	38	16	9	6
You have to describe the negative impacts posed by cybersecurity risks	29	34	17	13	7
You can name at least two warning signs that your device has been compromised	29	38	16	12	6
You have to describe the risks associated with storing information in personal clouds	29	32	20	10	8
You have to describe the risks in working from home for employees	28	37	17	11	7
You have to describe the risks associated with privileged users and standard users	27	32	22	10	9
You can identify a social engineering attack	25	30	26	9	19

Table 2. Employee confidence about Cybersecurity best practices (figures in %) [18]

2.5 Users' Behavior Towards Security

User's behavior seems to outflank technology-centric security every time. People tend to come up with unthinkable ways how to inadvertently compromise a solid security structure. A lack of comprehension of security threats and a drawback of industries in relation to security prioritization are unfolding dramatically and are becoming a major challenge these days.

The Analysis shows that 57% of employees believe that they would recognize if their device got hacked. This is alarming, given that many cybersecurity threats, including ransomware like Ryuk, can go undetected for months before detection by even the best organizations [19].

Employees must understand that there is a close relationship between what they do when using a computer or any other device at work and the risks their employer may face if the devices not used securely. Therefore, the relationship between quantity and quality of SAT should not be underestimated, and a deep understanding of security risks is essential.

Users' behaviour in regards to cyber threats will improve dramatically if an organization conducts Cybersecurity Awareness Training on a monthly basis [18].

Issue	*Once per month*	*A few times per quarter*	*Once per quarter*	*No more than Twice a year*
Clicking a suspicious link	60	46	49	44
Using a weak/simple password	51	46	47	42
Using the same password across systems	55	50	50	44
Leaving your device unlocked	51	51	42	37
Usage of public wifi hotspots without a VPN	51	49	46	47

Table 3. Correlation of Cybersecurity Awareness Training and various behaviors will result in a Malware Infection (figures in %) [18]

2.6 Stress in Cyber Security

Stress is an unpleasant, but inevitable professional hazard in cyber security.

When an organization has been hacked, the pressure is very intense and the cybersecurity professionals feel anxiety and can result in burnout. This is very destructive to physical and mental health of professionals and could have serious business implications [20].

The move of employees and IT teams to work from home as a result of COVID-19 has created even more challenges for cybersecurity teams that were already typically understaffed and working beyond their normal capacity. The statistics offer frightening evidence of the emotional impact of stress on cybersecurity [21].

The most dangerous and stressful situations arise when the risks are ambiguous. Therefore, it is extremely important to practice teamwork under pressure. The researchers found that what really mattered was less about who is on the team, and more about how the team worked together. The most important impact on team dynamics played psychological safety, where team members feel safe to ask, “what if” and no one will embarrass or punish anyone for asking questions or offering ideas [22]. A people-centric security culture enables psychological safety that allows employees to take risks and experiment without fear and retribution, and cultivate behaviors that lead to enhanced resilience.

2.7 Human behaviour under stress

Stress doesn't have to be extreme and leading to panic/impulsive decisions and outbreaks, but even a slightly elevated level of activation can already influence your cognitive processes and impact your rational thinking in a way that risk taking is increased and susceptibility is influenced.

There are few mechanisms and reactions of relevance in stressful (ambiguous) situations:

- Human cognition
- Group dynamics
- Organizational Culture

Human Cognition:

- Representativity heuristic – is a mental shortcut that people use when estimating probabilities. It involves making judgments by comparing things to concepts people already have in minds. The problem with this is that people often overestimate the similarity between the two things they are comparing [23].
- Confirmation bias – is a tendency for people to favour information that confirms their preconceptions or hypothesis regardless of whether the information is true [24].
- Consistency – individuals prefer that their thoughts, beliefs, knowledges, views, attitudes, and intents be harmonious, that is, that they do not contradict one another. Furthermore, these traits should be consistent with how people see themselves and their subsequent behaviors. Individuals will want change in order to establish congruency, relieve tension, and create psychological equilibrium, as inconsistency or asymmetry causes stress and undesirable psychological states [25].

Group Dynamics is a set of behavioural and psychological processes that occur within a social group or between groups. It refers to the "nature of groups, the laws of their development, and their interrelations with individuals, other groups, and larger institutions" [26].

Cognitive factors, group dynamics, and cultural boundaries can all make it difficult for the organization to recognize an ambiguous scenario. When these pressures combine, they establish a powerful mixture that makes it difficult to respond quickly to an uncertain threat [27].

Stress is usually a form of physiological arousal that is recognized and perceived as negative. From a biological point of view, the term "arousal" is more accurate, since it does not imply a person's awareness of an increased state of activation. Moderate arousal/stress increases the likelihood of cognitive distortions. The only way to sustainably mitigate them is to learn about them and develop "metacognitive awareness" to use cognitive control [28] [29].

Organizational security culture and processes can minimize the risk of stressful situations and increase the effectiveness of coping with them. Even if not all scenarios can be prepared for, regularly practicing low-probability but stressful threat scenarios improve metacognitive skills and team-level collaboration and communication.

2.8 Pipedrive's History and Culture

In 2010 the company was created with the focus to build a customer relationship management (CRM) tool to help businesses in their sales processes. The CRM tool helps with activity-based selling, meaning it is assisting in scheduling, completing, and tracking activities.

Over the years the company has created an environment with its own culture and core values. The six core values that makes this company unique can be seen through attitudes and behaviors, they are recognized and appreciated in many ways.

6 Core Values [30]:

- Be internally driven:
  You really love the work you do.
- Reach for Greatness:
  You break your own limits to explore what is possible, and venture into unknown territories.
- Don't ruin other people's days:
  In spite of your needs or frustrations at any given moment, there are no excuses for ruining someone's day.
- Be teachable:
  You are humble, and readily admit that you are not good at everything all the time.
- Put the team first:

Great things are achieved by teams, and you are accept that the team is collectively smarter than you.

- No excuses:
  When you hit an obstacle, you ask first what you can do to overcome it, instead of blaming others or the situation.

These are shared set of core values represent the unique culture of the company and can guide the decision-making process in variety situations which might relate to the security.

2.9 Financial Impact of Cyber Security Culture

Among the most effective approaches to justify the necessity for a security culture initiative is to demonstrate the financial impact of enhancing the culture. A Monte Carlo simulation technique is being used to evaluate the economic impact of security culture. Several assumptions have been made due to the lack of data currently available from Pipedrive regarding the financial costs of incidents.

Assumptions

Financial costs for security incidents: Minimum – 5,000 Euro (St. Dev 50); On average: 50,000 Euro (St. Dev 1000); Maximum: 250,000 Euro (St. Dev 10000)

The financial costs of security incidents include direct costs such as forensics analysis, financial penalties, reimbursement, indirect costs such as lost profits due to system downtime, communication costs, efforts to get accounts back in operation, and lost opportunity costs such as loss of prospective customers, damaged reputation and, as a result, lost revenue and loss of competitive advantage in the market.

Security Culture Strength:

Weak: 80% likelihood of making a wrong security decision; Moderate: 50% chance of making a poor security judgment; Strong: 20% chance of making a poor security choice.

Actual Data

Number of bugs and security failures last year in Pipedrive: 288 (St. Dev 5)

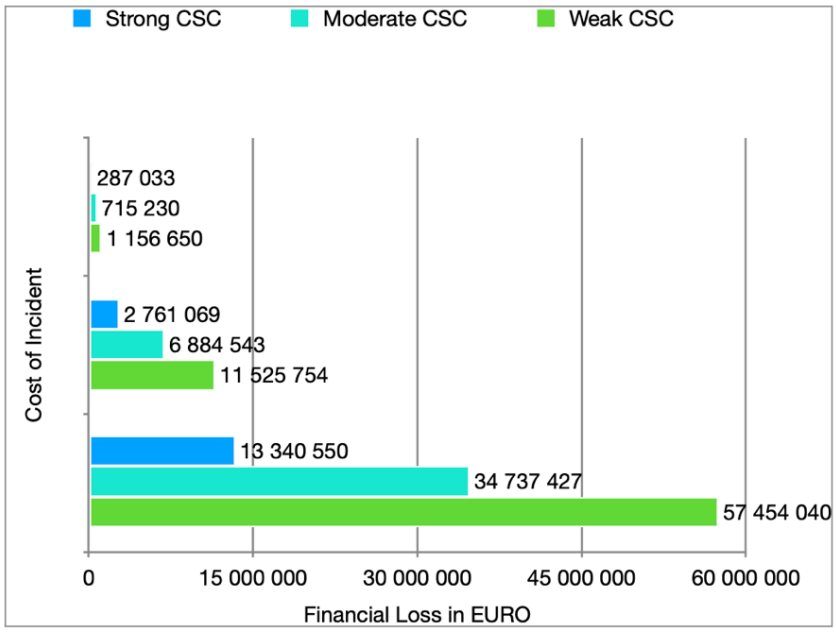

Figure 3. Monte Carlo simulation results, annual incident losses based on the strength of security culture.

As shown in Figure 3, the financial consequences of a weak security culture can be catastrophic. With a weak security culture, annual losses can reach 57,454,040 euros if 80% of security decisions, bugs, failures lead to security incidents. The annual loss with a strong security culture could be €13,340,550, which is a significant difference from the financial loss with a weak security culture.

The result of this model shows that the security culture transformation project has the potential to save Pipedrive millions of euros.

3 Methodology

Cultural transformation in an organization cannot be accomplished without commitment, communication and hard work. It is necessary to understand the challenges associated with changing corporate culture and implement key strategies. The cultural transformation must include everybody, from top to bottom and there must be set in place a continued assessment of the current culture.
The assessment is crucial for the achievement of security culture and changes in behavior.

3.1 Concepts and Measures

The case study for this research is the security culture in Pipedrive. This includes evaluating the metric values in connection to coherent key behaviors, as well as measuring and analyzing the current security culture and investigating the security behavioral model to contribute meaningfully to an organization's security culture transformation. Pipedrive currently has over 900 employees and the number continues to grow. The author goal was to get at least 500 participants although the maximum number of opinions can give more precise overview of the existing security culture.

3.2 Theory

As a quantitative method of researching data on the existing security culture, the author used two surveys and one value metrics.
Both surveys were used to examine the existing security culture in Pipedrive and to confirm or refute the tentative hypothesis that a Trust Culture is dominant in Pipedrive, according to definition in CSCF [2]. Based on Pipedrive's fundamental principles that every individual is valuable and contributes to the company's success, this is very much in accordance with the Trust Culture (CSCF), which values people based on their talents to contribute to the shared goals rather of their title or position [2].

3.3 Security Culture Survey Data collection

The survey was conducted using Alchemer tool and distributed to all Pipedrive employees. The rationale for use quantitative research method is justified in such a way that in a short period of time we can get concise survey from the maximum number of people willing to fill it out. Participants were given 15 minutes to fill in the survey and 294 employees responded and fully completed.
Clear instructions regarding completion of the questionnaire, confidentiality, anonymity and voluntary participation were provided. Three (3) weeks was used to collect the data for the study.

The Security Culture Diagnostic Survey adopted an ipsative scale to measure answers, with ten questions and four responses that were to be assigned a score of ten points, divided among the responses according on how strongly or weakly each statement represents the organization. The author utilized SCDC questions developed for CSCF by Hayden, Lance (full questionnaire in Appendix) [2].
Participants were required to indicate the number of years they had been in the Pipedrive and also the department and, if it exists, then the sub-department in which they work.

U**nderstanding the questions**

The SCDS is comprised of 10 questions that correlate to core organizational activities influenced by information security culture behaviors. The response options help to categorize the organization's security culture into four CSCF quadrants [2].

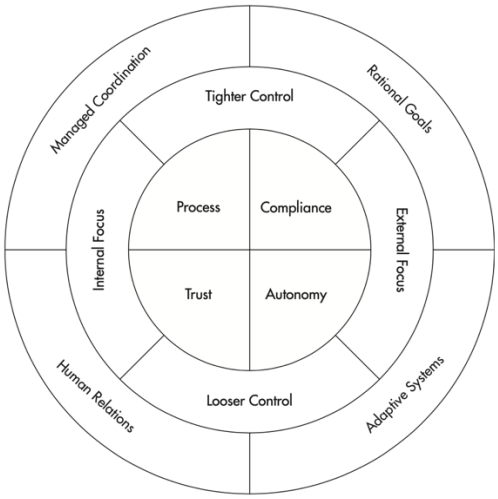

Figure 4. The Competing Security Cultures Framework (CSCF)

Each response describes traits, values and activities that associated with one of the CSCF quadrants [2]:

"**A**" - internally facing and prioritize tighter control.

"**B**" - prioritize tight control, but are aimed at external stakeholders.

"**C**" - externally facing, but prioritize less control over decisions and activities.

"D" - internally facing and more loosely controlled

To proper analyze the results, it is important to understand the questions of the survey [2]:

Question "What's Valued Most?" allows to reflect on the core values that influence the organization's security culture and identify priorities in day-to-day decision-making.

Question "How Does the Organization Work?" helps to see how the organization fulfills its objectives, how it shares responsibility and authority, and how it implements these values in hierarchies.

Question "What Does Security Mean?" allows to understand how the respondent conceptualize information security.

Question "How is the Information Managed and Controlled?" helps to identify information management and control as a common resource.

Question "How are Operations Managed?" allows to prioritize the organization's daily functional activities, interactions, and resolutions.

Question “How is Technology Managed?” helps to identify whether technologies are subject to oversight and used to benefit the organization.

Question “How are People Managed?” allows to uncover how people treated and their resourcefulness.

Question “How is Risk Managed?” helps to collect information about how employees understand risk management.

Question “How is Accountability Achieved?” allows to see how accountability is perceived within the organization.

Question “How is Performance Evaluated?” focuses on understanding, whether measurements of success or failure defined.

3.4 Security FORCE Survey Data Collection

The survey was conducted using Alchemer online tool and distributed to all Pipedrive employees 2 weeks after the completion of the Security Culture Survey. Participants were given 10 minutes to fill in the survey and 372 employees responded and fully completed. Clear instructions regarding completion of the questionnaire, confidentiality, anonymity and voluntary participation were provided. Two weeks was used to collect the data for the study.

Participants were required to indicate the number of years they had been in the Pipedrive and also the department and, if it exists, then the sub-department in which they work.

A Likert scale with a range of opinions (from "Strongly Disagree" to "Strongly Agree") was used in the Security FORCE Survey to provide a sequence of answers that go from one extreme to the other with less extreme choices in the middle. The Likert scale provides a range of answers that can be used to assign numeric value to survey responses, such as 1 through 5, and to determine the mean levels of agreement throughout all survey respondents. The author utilized FORCE Survey questions developed by Hayden, Lance (full questionnaire in Appendix) [2].

For example:

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Security Value of Failure					
1. I feel confident I could predict where the organization's next security incident will happen.					

Table 4. Sample of the FORCE survey [2]

3.5 FORCE Metrics Data Collection

In the Security FORCE Metric values were collected from the Management of Information Security Team and include values such as number of security failures; average time to handle operational issues; amount of official non-security stakeholder assessments of security plans in the previous year; number of personnel having security roles written into their job descriptions, and so on. The author utilized FORCE Metrics questionnaire developed by Hayden, Lance (full FORCE Metrics questionnaire provided in Appendix) [2].

The FORCE Metrics Model includes 25 measures, and each result of a specific metric is associated with a key value behaviour of the FORCE Model.

For Example:

Security Value of Failure	Results	Key Value Behaviours
1. Number of security failure scenarios developed in the past year.	>->	Anticipate failures
2. Number of security failures (whenever or not resulting in a formal security incident) reported in the past year.	>->	Seek out problems
3. Ratio of security incidents with no prior failure reporting or indicators in the past year.	>->	Reward problem reporting
4. Ratio of security failure or incident data (reports, root-cause analyses, after-actions, etc.) voluntarily shared outside the information security program.	>->	Share information about failure
5. Ratio of security failures resulting in system changes.	>->	Learn from mistakes

Table 5. Sample of FORCE Metrics and Key value Behaviours [2]

3.6 Methods of Data Analysis

It is important to understand people perception on security, their worries and willingness to learn and implement their new knowledge. Questions were used primary to analyze

and to explore the major challenges that all employees face with regard to cyber security awareness, as well as to understand the correlation of key organizational activities that are influenced by behaviors that are central to information security culture.

The quantity of data was sufficient to carry out a thorough analysis.

Based on the collected data from the Security Culture Survey, different teams within the organization will be compared and evaluated to identify the dominant culture and existing subcultures. The existing culture will also be compared among new employees and employees that have been with Pipedrive for more than 3-5-7 years to see how culture evolves over the years.

Based on the collected data from the FORCE Survey, security behavioral traits in Pipedrive will be examined and adaptation to people-centric security changes will be evaluated.

In addition to the Security FORCE Survey, relevant value metrics will be evaluated to assess how close they are to the Highly Reliable Security Program's associated traits [2].

4 Analysis

The aim of this chapter is to analyse the survey in order to create guidelines for transformation to the desired security culture. The author used Alchemer tool and created charts and histograms in Numbers to visualze the collected data.

4.1 Summary of existing Security Culture

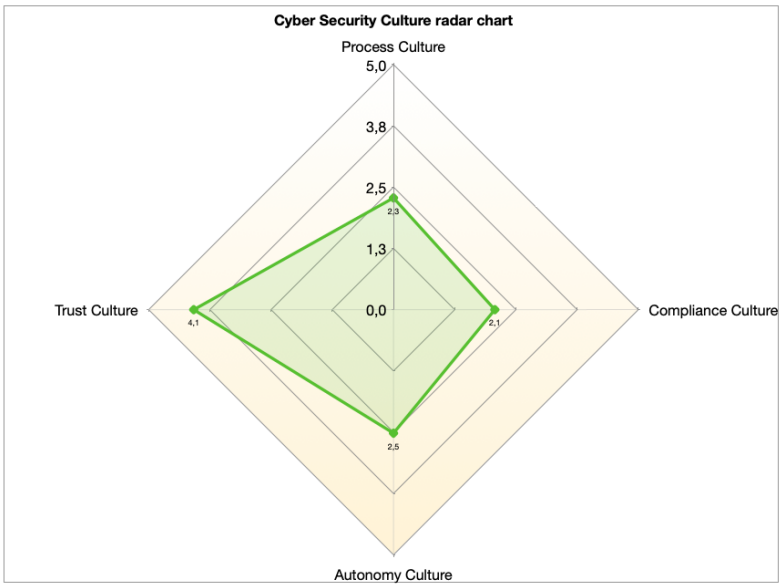

Figure 5. Summary of existing Security Culture

Pipedrive's responses revealed a few important things. The highest scores were given to "D" responses, which correspond to the Trust Culture based on the CSCF. The average score is 4.1, which is 37,3% from all the cultures. This indicates less control and more shared responsibilities, allowing people to think for themselves. Team collaboration and mutual accountability are valued and prioritized in the workplace.. Employees have mutual support, respect and a strong sense of community that encourages them to share successes and failures. The departments with the highest scores for Trust Culture responses are Channel and Partnerships (50%), Product Design (44,8%), and Support (43,6%). The departments with the lowest scores for Trust Culture responses are Information Security (30,1%) and IT Ops (28,1%). Although in the big picture we see that security departments have the lowest scores for trust culture responses,

nevertheless, based on the percentage distribution across cultures, trust culture still scores the highest. This means that Pipedrive's security experts do not view humans as threat actors, but rather strive to provide them with the greatest tools to make the proper security choices, and they place a high emphasis on human development in security awareness.

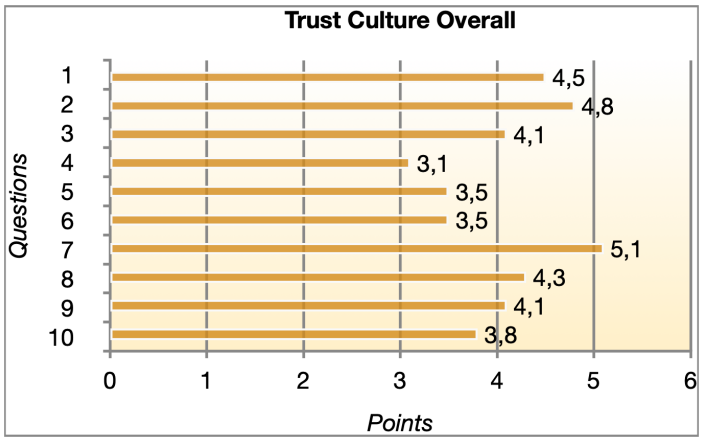

Figure 6. Trust Security Culture scores

The greatest discrepancies appeared in the answers "A", that belong to Process Culture. The average score is 2.3, which is 20,8% from all the cultures. A Process Culture values the stability of existing functions, the visibility of established processes, and the standardization of operations. For optimization, hierarchical structures with areas of responsibility and defined processes are created. Tight control of security activities throughout the organization is essential. The departments with the highest scores for Process Culture responses are IT Ops (25,%) and Customer Success (22,1%). This means that these departments measure their performance according to how well their operations are handled and organized, and they expect centralized management to assure uniformity across all operations.

The departments with the lowest scores for Process Culture responses are Channel and Partnerships (6%), Business Intelligence (17,2%) and Product Design (16,4%). This indicates that these departments tend less towards centralization and bureaucratic lines of control, where policies and procedures are not prioritized values.

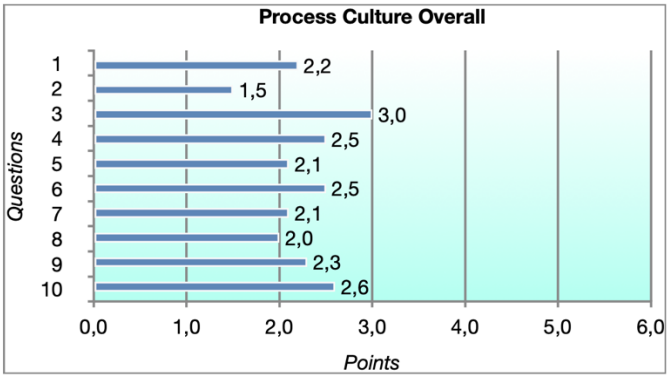

Figure 7. Process Security Culture score

Interestingly, the lowest response scores were given to “B” responses, which stands for Compliance Culture in the CSCF. A compliance culture values conformity to external expectations, repeatability to provide results upon request, and documentation to hold evidence and fulfill the obligations of others. The department with the highest scores for Compliance Culture responses is IT Ops (24%).

However, in question 3 "What does 'security' mean in Pipedrive?" The Department of Information Security gave the highest score to the answer "B", which means that they, like the IT Operations Department, are often involved in compliance activities such as external security audits and are committed to complying with various ISOs.. The departments with the lowest scores for Compliance Culture responses are Business Intelligence (10,6%) and Channel and Partnerships (10,5%). This demonstrates that these departments are not bound by the demands of external stakeholders, such as customers or regulatory organizations.

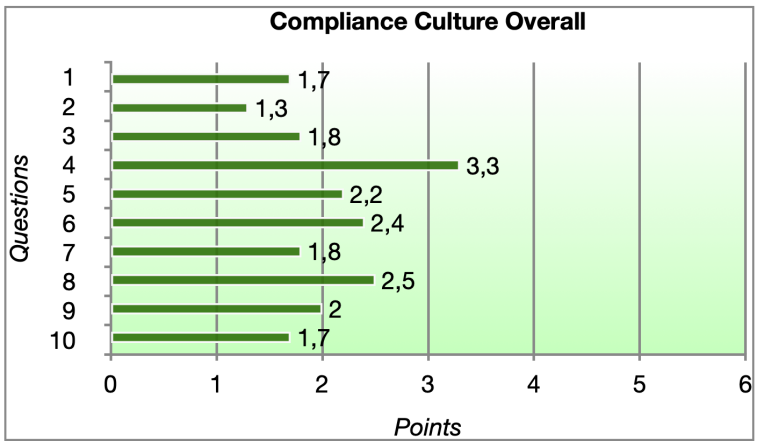

Figure 8. Compliance Security Culture scores

The responses associated with “Autonomy Culture” corresponds to “C” responses received the second highest percentage in overall assessment, which is 23%. The Autonomy Culture is a culture based on the principles of "getting results", where the organization values maximum flexibility, agility and innovation, and a cautious approach to security can lead to failure in a competitive environment. Individually or locally managed security is preferred over centralised security, so security authority and responsibility could be distributed throughout autonomous divisions. The Autonomy Culture can be seen in the BYOD movement, where employees can use their devices and phones to access the corporate network. The degree of Autonomy Culture within Pipedrive can affect the way BYOD is managed and determine the security risk tolerable.

The departments with the highest scores for Autonomy Culture responses are Channel and Partnerships (33,5%), Information Security (30,1%) and Business Intelligence (31,2%). This reveals that the Department of Information Security places great value on individual understanding of security and responsibility, the ability to keep pace and stay ahead of progress, instead of prioritizing standard processes of centralized security management. Often tech startups have the highest culture of autonomy because they are growing so fast that information security needs to be handled by individuals or locally created entities. The departments with the lowest scores for Autonomy Culture responses are Support (16,7%) and Customer Success (20,6%). The Autonomy Culture responses reflect externally facing values and traits, this demonstrates that the departments with the lowest scores are less lenient on business agility than the rest of the departments in Pipedrive.

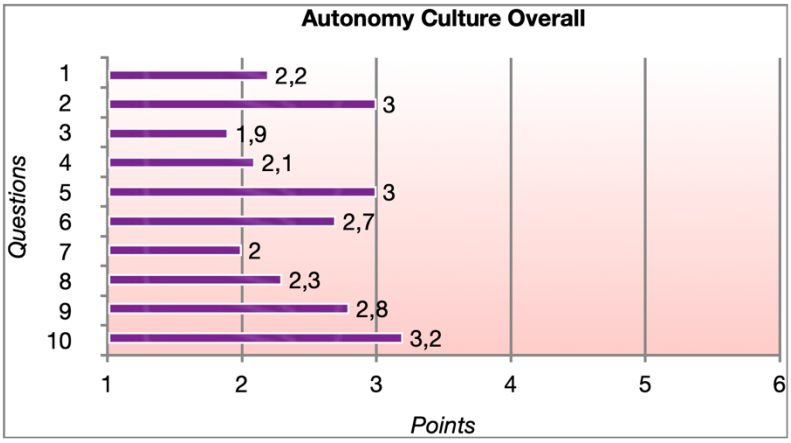

Figure 9. Autonomy Security Culture scores

4.2 Cyber Security Culture by Departments

For a detailed analysis, it is useful to look at each answer to understand why one or another received a higher score and which values are most favourable and least favourable. It also helps identify critical areas that need to be addressed and areas of strength that can be used to help develop an action plan. Detailed analysis for all departments and a summary of the analysis for each department can be found in Appendix.

4.3 Engineering Sub-Departments Comparison

Engineering Operations - 70 employees, received 28 responses, which is 40% and acceptable response rate.
Engineering Platform - 17 employees, received 13 responses, which is 76% and acceptable response rate.
Software Development - 285 employees, received 74 responses, which is 25% and acceptable response rate.

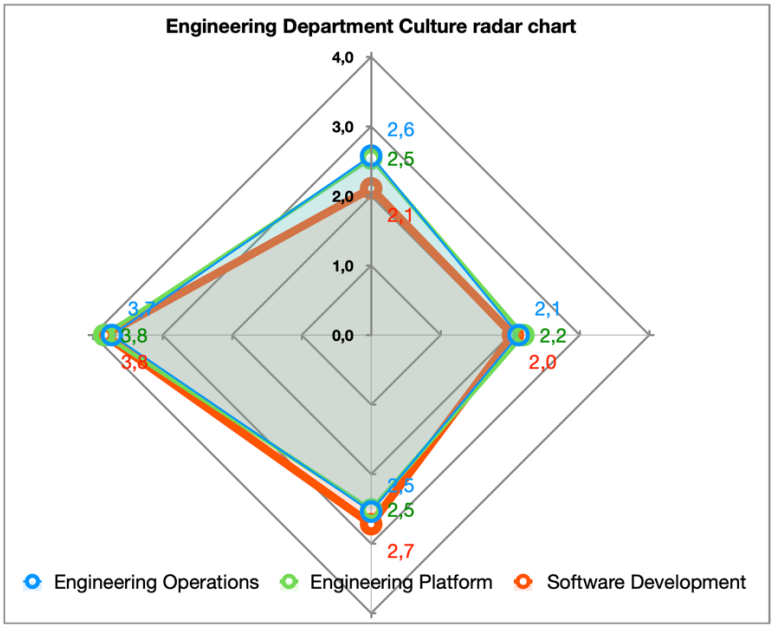

Figure 10. Engineering Department Culture radar chart

The dominant security culture present in these departments is the Trust Security Culture, accounting for 34% to 35.8% of all other existing cultures. This indicates that people put a lot of themselves into teamwork. Human relations, collaborative processes

and shared security play a central role in these Engineering sub-departments. People are seen as security advocates, not threats.

The next dominant culture is the Autonomy Security Culture, which accounts for 22.7 to 25.4% of all other existing cultures. This culture shows that people see value in individual autonomy when they can make their own security or any other decisions. It is important to note that Software Development department has the highest average percentage of 25.4% and means that freedom in decision-making and innovation are most valued in this team.

The next introduced culture is Process Security Culture, which accounts for 19.7% to 23.5% of all other cultures. Some of the values of this culture compete with the Autonomy Security Culture's values. These percentages indicate that centralized management, policies, and procedures are also important to Engineering Departments. However, in the Software Engineering department, the Process Culture percentage is 3.8% less than the highest percentage, and for the Autonomy Culture, it is 2.7% higher. This reveals that people in the Software Development department believe that flexibility, and agility are more beneficial to success and growth than standardization.

The culture with the lowest percentage, ranging from 19.1% to 19.8% of all other cultures in existence, is the Compliance Security Culture. This shows that compliance requirements from external parties in the engineering department are limited and it is possible that security issues related to concerns of other stakeholders, whether customers or regulators, may not be directly relevant to them, or perhaps that majority of people in this department are not involved with external regulation and audit reports.

4.4 Comparison of Security Culture by Tenure

In this chapter, the author aims to find out how Security Culture changes depending on the length of stay of employees in the Pipedrive.

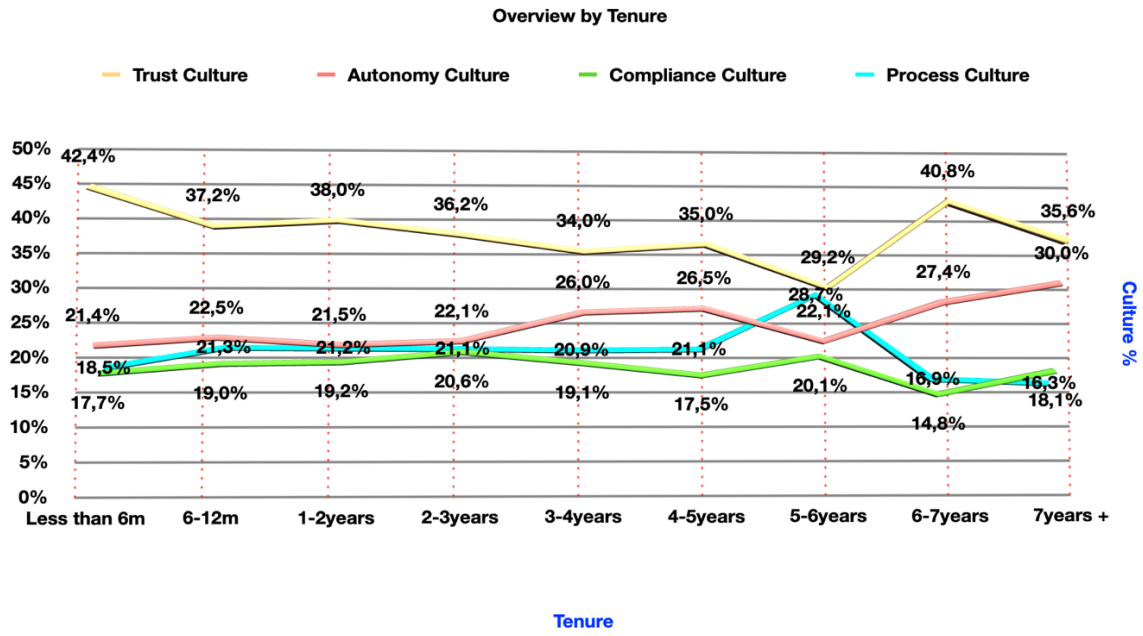

Figure 11. Security Culture overview by Tenure

As comes from Figure 11, overall, regardless of tenure, the dominant Security Culture for all is the Trust Security Culture, ranging from 29.2% to 42.4%. This culture indicates the importance of a supportive community and sense of a family, opportunity and development, teamwork and collaboration to achieve common goals. In terms of security, this culture also means shared responsibility and a great deal of trust in people's experience, therefore human relationships play a very crucial role. People are seen as security guards, not threats.

The highest percentage of Trust Security Culture at 42.4% is present in employees with the shortest tenure, i.e. less than 6 months. Such a high percentage shows that newcomers go through a period of onboarding and learning where they feel a lack of personal responsibility and mostly experience shared responsibility and teamwork. The Compliance Culture is the least present, only 17.7%, perhaps due to the fact that newcomers are not yet familiar with all the requirements and external audits. The next existing culture at 18.5% is the Process Security Culture, which is also a fairly low

percentage and indicates that formal and bureaucratic procedures are underrepresented. The Autonomy Security Culture corresponds to 21.4%, which means that freedom, flexibility and innovation are preferable to strict policies and centralized control.

The Trust Security culture has a fairly large drop of 8.2% for employees with tenure between 6 months and 1 year, from 42.4% to 37.2%, while there is a concurrent percentage increase in the other three existing cultures. The Autonomy Security Culture increases by 1.1%, from 21.4% to 22.5%, the Process Security Culture increases by 2.8%, from 18.5% to 21.3% and the Compliance Security Culture increases by 1.3%, from 17.7% to 19%. This shows that there is a fairly large shift in values, day-to day activities, comprehension of responsibilities and performance evaluation. Employees with 6 months to 1 year of tenure face more standardization and formalities, possible external review and encouragement of innovative solutions.

There is little change of less than 1% for all Security Cultures for employees with tenure between 1 year to 2 years. A slight increase is observed in the Compliance Culture, by 0.2% and by 0.8% in the Trust Culture. The Autonomy Culture and Process Culture decreased by 1% and by 0.1%, respectively.
Similarly, there is the smallest decrease present in the Process Culture by 0.1% for employees with tenure between 2 to 3 years. For employees with the same tenure, the result for the Trust Culture is a drop of 1.8%, which demonstrates a decrease in cooperation and an increase in individual action, flexibility in decision-making and increase in external regulations due to an increase in Autonomy Culture by 0.6% and in Compliance Culture by 1.4%.

It is interesting to note, as can be seen from Fig 11 that for employees with tenures ranging from 6 months to 2-3 years, Security Cultures have only minor variations, hardly exceeding 1% variation, such stability in values and behavior means that there is a certain framework of cultural existence which were installed 2-3 years ago. According to open sources, Pipedrive was acquired by Vista Equity Partners two years ago, in 2020 [https://mergr.com/vista-equity-partners-acquires-pipedrive], which have affected the cultural behavior of new hires who joined Pipedrive at the time of this transition. Also, this indicates that the 193 employees with tenure from 6 months to 2-3 years who took part in the survey, and joined during the transition or after it, have a fairly consistent

view of Pipedrive's security culture. However, it also shows the period of the Covid-19 pandemic, so this could be a factor influencing key behavioral values.

The results for employees with 3 to 4 years of tenure show a continuing decline in Trust Culture by 2.2%, from 36.2% to 34%. While the Trust Culture declined, the Autonomy Culture increased, by 3.9% from 22.1% to 26%, which is a significant change. Perhaps this is the result of gaining more experience and gaining more freedom of action, where personal responsibility also increases, but at the same time shared responsibility decreases. There is little to no change in Process Culture for employees with this tenure, only a slight decrease of 0.2% from 21.1% to 20.9%. Compliance culture also saw a 1.5% decrease, from 20.6% to 19.1%. This indicates an association with an increase in the Autonomy Culture, where innovation is encouraged, and a corresponding decrease in the Compliance Culture, where standard behaviour is favoured.

The data for employees with 4 to 5 years of tenure, show present a fairly stable Process Culture, increasing slightly by 0.2%, from 20.9% to 21.1% and getting to the same level as for employees with 2 to 3 years of tenure. This means that formal and bureaucratic processes and centralization are constantly in the same range for the majority of employees, i.e. 281 people who took part in the survey, and who have worked in Pipedrive from 6 to 12 months and up to 4-5 years, which shows that there are smooth, predictable activities and satisfactory visibility of operations. Also, for these employees, the Compliance Culture is reduced by 1.6%, from 19.1% to 17.5%, as a result of which the level of Compliance Culture for them is even lower than the level that existed for an employee who had just started working. Trust Culture and Autonomy Culture slightly increased for employees with 4 to 5 years of tenure, now it is 35% and 26.% respectively.

As follows from Figure 11, for employees with 5 to 6 years of tenure, there are quite noticeable differences in the existing levels of Security Cultures compared to other employees with shorter tenure. For these employees, the Trust Security Culture has the lowest percentage, at 29.2%, of all other short- or long-term tenures. Process Culture has 28.7% and is the highest percentage which indicates the importance of stability in operations, transparency in documentation and preference for a centralized security function to oversee the entire organization. The Compliance Culture for these

employees is also one of the highest at 20.1% compared to other employees with other seniority, excluding employees who have been with Pipedrive for 2 to 3 years, they have a Compliance Culture at 20.6%. The Autonomy Culture is 22.1%, which reveals a decrease in percentages compared to 4-5 years and 6-7 years in office, 26.5% and 27.4% respectively, this means quite large changes in behavior associated with this culture, such as having less unexpected decisions and achieving results are not above the rules. The priorities for them are more in line with the values and behavior of the Process Culture, where security shows more standardization, policies and procedures, and the implementation of technology to protect information assets.

For employees with 6 to 7 years of experience, Trust Security Culture is more than double the Process Culture and Compliance Culture, at 40.8%, the highest after employees with less than 6 months of experience with Pipedrive. The author should point out that 8 highly tenured employees took part in the survey, and such a surge in a Trust Culture reveals that they have a strong sense of belonging and a "feeling at home". Perhaps these employees demonstrate high commitment, trust, and hope for their work environment because they have developed affective bonds with Pipedrive. The Autonomy Culture is also quite high for these employees, 27.4%, where freedom is highly valued and one can make independent decisions without hesitation, having the necessary experience and knowledge. The Process Culture and Compliance Culture among these employees is the least present, these are 16.9% and 14.8%, respectively. These are also the smallest percentages compared to other short or long tenure. Except that the Process Culture is even lower for employees with work tenure of 7 years or more - 16.3%. The explanation is that these people were at the origins of the creation of Pipedrive, then a limited number of people worked and they were mainly teams of experts whose goal was to achieve the best results, and not to focus on bureaucratic documentation and external checks. It is possible that these people still retain and have similar cultural values and behaviors.

As can be seen from Figure 11, for employees with more than 7 years of tenure, a Trust Culture still dominates, although it has declined significantly by 5.2% compared to employees with 6 to 7 years of tenure. The Autonomy Culture has the highest percentage of 30% among all other employees with different tenure. It is noteworthy that there is a gradual increase in the Autonomy Culture, starting from the shortest

tenure of 21.4%, all the way up to 30% for employees with 7 and more years of tenure, except for employees with a tenure of 5 to 6 years, where it is reduced by 4.4 % to 5.3%. The Compliance Culture at 18.1% is also low for these employees and demonstrates less anxiety about showing the evidence of visibility and control to parties outside of Pipedrive.

The Process Culture of these employees has one of the lowest rates - 16.3%, which is due to the same reasons as those of employees with 6 to 7 years of work tenure.

4.5 FORCE Survey Analysis

The aim of this chapter is to analyse the Security FORCE survey to determine how the organisation's behaviours is in line with that of the HRSP (Highly Reliable Security Program) and to support Security Culture transformation.

It is important to note that results of the survey cannot be a single point of judgment whatever or not Pipedrive operates as an HRSP. Therefore, it is necessary to carry out ongoing evaluations over time in order to be able to evaluate and compare multiple data points.

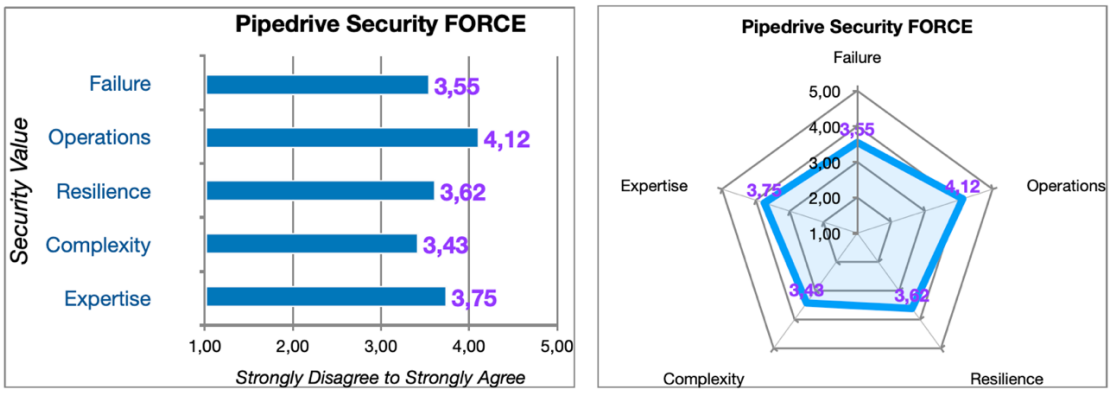

Figure 12. FORCE results overview

Figure 12 depicts the total results of the Pipedrive Security FORCE survey, where for side-by-side comparison and shape comparison, a histogram and spider chart with all five value scores are shown.

The analysis is performed based on the scoring of each FORCE value and presents the following associated statements [2]:

- An average score of 4 or above (majority of responses are Agree or Strongly Agree) indicates that the Pipedrive exhibits HRSP-like behaviors.
- An average score of 3 (majority of responses imply that the respondent felt Neutral) indicates that the Pipedrive may or may not act like an HRSP.
- An average score of 2 or less (majority of responses are Disagree or Strongly Disagree) implies that the Pipedrive does not display HRSP-like behavior.

Pipedrive's responses revealed the following important findings.
The highest scores were given to **Security Value of Operations**, with an average score of 4.12. This reveals that most responses received Agree or Strongly Agree, implying that Pipedrive behaves like an HRSP.

	Statements	Key Value Behaviours	Grand Total
6	I know that someone is constantly keeping watch over how secure Pipedrive is.	• Keep your eyes open	4,39
7	I am confident that information security in Pipedrive actually works the way that people and policies say it does.	• Form a bigger picture	4,08
8	I feel like there are many experts around Pipedrive willing and able to help me understand how things work.	• "Listen" to the system	4,38
9	Management and the security team regularly share information about security assessments.	• Test expectations against reality	3,90
10	Management stays actively involved in security and makes sure appropriate resources are available.	• Share operational assessments	3,84

Figure 13. Security Values of Operations overview

It is critical to examine the survey itself for a more complete analysis, in Figure 13, statements 6 through 10 refer to the Security Value of Operations and have the corresponding key behavior next to them. Key behaviors associated with HRSP that maximize the security of operations and are used to learn more about what is actually happening in Pipedrive. Technology and infrastructure are part of operational activities, as are many other elements including human interactions, policies, and plans.
Statements with a mean number of 4 or greater demonstrate that Pipedrive acts like an HRSP, that it recognizes how things function in a security environment, and that it has mechanisms for detecting faults that might result in failure. Because of the greater operational awareness, the Pipedrive can identify even the smallest faults. Interesting to note the departments with the lowest scores, below 4, for Security Value of Operations are Business Intelligence, Information Security, Finance and Product Org. As for the Information Security department, this indicates some inconsistencies in terms of operational readiness and can be further verified using FORCE Metrics.

The next highest scores were given to **Security Value of Expertise**, with an average score of 3.75. This shows that most responses received Neutral or Agree and implies that Pipedrive may or may not act similarly to HRSP.

	Statements	Key Value Behaviours	Grand Total
21	I know exactly where to go in Pipedrive when I need a expert.	• Ask the experts	3,87
22	I think everyone in Pipedrive feels that monitoring security is part of their job.	• Suppress the ego	3,74
23	In the event of a security incident, people can legitimately bypass the bureaucracy to get things done.	• Allow authority to migrate	3,27
24	People in Pipedrive are encouraged to help other groups if they have the right skills to help them.	• Share credibility	4,19
25	I feel empowered to take action myself, if something is about to cause a security failure.	• Reward calls to action and cries for help	3,67

Figure 14. Security Values of Expertise overview

As seen in Figure 14, statements 21 through 25 refer to the Security Value of Expertise and have a corresponding key behavior next to them. The HRSP-related core behaviors outlined optimize the security value of expertise while also making Pipedrive more adaptable and agile in the case of cybersecurity threats or even never-before-seen disasters. HRSPs enjoy the benefits of the security value of expertise in situations when authorities have to be more adaptable in order for decisions to be made by those who are nearest to the situation and most informed on how to handle it. Statements where the average value is 4 or higher indicates that Pipedrive acts like an HRSP and allowing the authority to respond and integrate with the expertise required to produce appropriate decision in critical circumstances. However, only one statement met this score, the remaining four statements received an average value of 3 or greater, indicating that Pipedrive prone to encounter adaptability issues in some situations and in some departments. The departments with the lowest scores, below 3.5 for the Security Value of Expertise are People & Culture, Business Intelligence, Finance.

The next highest scores were given to **Security Value of Resilience**, with an average score of 3.62. This reveals that most responses received Neutral or Agree and implies that Pipedrive may or may not behave like HRSP.

	Statements	Key Value Behaviours	Grand Total
11	I feel like people are trained to know more about security than just the minimum level necessary.	• Overtrain people	3,63
12	Pipedrive has reserves of skill and expertise to call on in the event of a security incident or crisis.	• Create "Skill benches"	4,06
13	I feel like everyone in Pipedrive is encouraged to "get out of their comfort zone" and be part of security challenges.	• Actively share expertise	3,53
14	I feel like people are interested in what I know about security, and willing to share their own skills to help me as well.	• Encourage stretch goals	3,48
15	Pipedrive often conducts drills and scenarios to test how well we respond to security incidents and failures.	• Practice failing	3,39

Figure 15. Security Value of Resilience overview

As seen in Figure 15, statements 11 through 15 refer to the Security Value of Resilience and have a corresponding key behavior next to them. The HRSP-related key behaviors presented optimize the security value of resilience, allow Pipedrive to be ready for any disruption and be prepared to respond, adapt and continually learn from incidents to minimize their impact. The Security Value of Resilience relates to the ability of the Iinformation security program to skillfully and professionally deal with big security events, where the experience is stressful for all parties concerned, but the incident is managed in a way that Pipedrive becomes much stronger. Statements with a mean number of 4 or above imply that Pipedrive acts like an HRSP and can address to security events faster and efficiently. This demonstrates that the resources and systems required to cope with unforeseen situations are in place. However, only one statement received this score, which means that only 20% of the time Pipedrive acts like an HRSP, the other four statements received an average value of 3 or higher, demonstrating that Pipedrive has trouble recovering swiftly after a security breach and also have problems controlling the failure mechanism. The departments with the lowest scores, below 3.5 for the Security Value of Resilience are Information Security, People & Culture, Product Research.

The next highest scores were given to **Security Value of Failure**, with an average score of 3.55. This reveals that most responses received Neutral or Agree and implies that Pipedrive may or may not behave like HRSP.

	Statements	Key Value Behaviours	Grand Total
1	I feel confident I could predict where Pipedrive's next security incident will happen.	• Anticipate failures	2,23
2	I regularly identify security problems while doing my job.	• Seek out problems	2,79
3	I feel very comfortable reporting security problems up the management chain.	• Reward problem reporting	4,20
4	I know that security problems I report will be taken seriously.	• Share information about failure	4,35
5	When a security problem is found, it gets fixed.	• Learn from mistakes	4,17

Figure 16. Security Value of Failure overview

As seen in Figure 16, statements 1 through 5 refer to the Security Value of Failure and have a corresponding key behavior next to them. The HRSP-related core behaviors presented optimize the security value of failure, enable Pipedrive to learn from failures, and so discover errors and mistakes as soon as possible when they are still still tiny and easy to fix. The Security Value of Failure refers to the ability recognise failures as the most valuable security resource. Even small failures can provide symptomatic clues that something is wrong or not functioning properly and can be an opportunity to address it promptly. Pipedrive performs like an HRSP and is more capable of learning from failures and establish optimal conditions for disclosing security vulnerabilities, according to statements with an average value of 4 or above. There are three statements that score above 4, which means that only 60% of the time Pipedrive behaves like an HRSP. However, there are two statements with the lowest scores, 2.23 and 2.79, indicating that Pipedrive not be able to detect minor failures and therefore be unable to prevent a major incident. The departments with the lowest scores, below 3.5 for the Security Value of Failure are Business Intelligence, Marketing, People & Culture, Product Design and Product Research.

The next highest scores were given to **Security Value of Complexity**, with an average score of 3.43. This reveals that most responses received Neutral or Agree and implies that Pipedrive may or may not behave like HRSP.

	Statements	Key Value Behaviours	Grand Total
16	I feel like people in Pipedrive prefer complex explanations over simple ones.	• Don't oversimplify	2,70
17	I feel like people are open to being challenged or questioned about how they arrived at an answer.	• Formalize your assumptions	3,69
18	Pipedrive always has plenty of data to explain and justify its decisions.	• Covet empirical evidence	3,65
19	People from outside the security team are encouraged to participate and question security plans and decisions.	• Share the doubt	3,45
20	Pipedrive formally reviews strategies and predictions to make sure they were accurate, and adjusts accordingly.	• Make every model better	3,64

Figure 17. Security Value of Complexity overview

As seen in Figure 17, statements 16 through 20 refer to the Security Value of Failure and have a corresponding key behavior next to them. The HRSP-related core behaviors given optimize the security value of complexity, enable Pipedrive to maintain a critical inner attitude, and push itself toward more comprehensive and sophisticated explanation techniques. Complexity is fundamental to reliability, and oversimplification creates unnecessary risk, which is why HRSP highlights the importance of hidden aspects that can potentially destabilize the ability to respond to threats. There are no statements with and average score of 4 or higher, which corresponds to HRSP behaviour. There are four statements with an average score of 3 and above show that Pipedrive have limited collaboration on information security decisions and there is also insufficient evidence and reviews of the effectiveness of existing security models, frameworks to assess their relevance and accuracy. Additionally, a single statement with an average score of 2.70 shows that Pipedrive is likely oversimplifying the security program's problems and indicating the presence of potentially dangerous blind spots. All departments score below 3.5 on the Security Value of Complexity, with the exception of two, the Executive and Support departments.

4.6 FORCE by Tenure

In this chapter, the author aims to find out how the Security FORCE Values change depending on the length of time employees stay in Pipedrive.

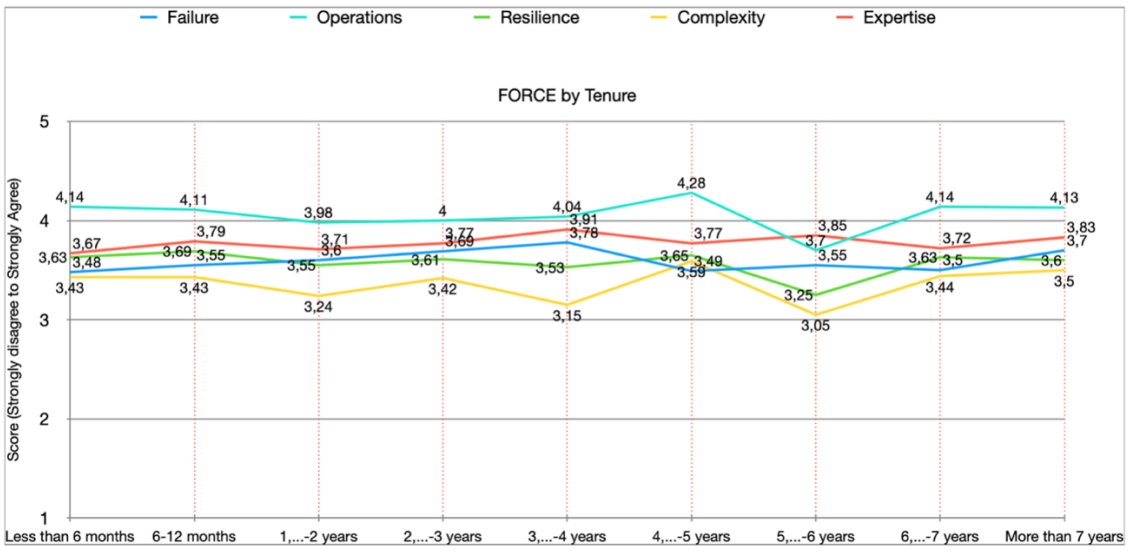

Figure 18. FORCE results by Tenure

As shown in Figure 18, the vast majority of employees rated above 4 on the Security Value of Operations, which is in line with HRSP behaviours, with the exception of employees who worked for Pipedrive for 1 to 2 years with an average score of 3.98 and for 5 to 6 years with an average score of 3.7. This demonstrates that the majority of employees believe Pipedrive is acting in a manner that optimizes the security value of operations and is well-equipped to find flaws and preserve operational visibility. It is interesting to note that the Security Value of Complexity has received average scores in the range of 3.0-3.50, which is the lowest score among almost all employees, except for those with 4 to 5 years of tenure, where the score is 3.59. In this situation, low scores indicate that Pipedrive staff prefer oversimplification in the cybersecurity ecosystem, resulting in a lack of data, metrics, and maybe outdated frameworks to back decisions. All security values are in the same sequence and are relatively close in value for employees with less than 6 months, 6 to 12 months and also 6 to 7 years of tenure. Where the value of Complexity ranges from 3.43 to 3.44, the value of Failure ranges from 3.48 to 3.55, the value of Resilience is from 3.63 to 3.69, the value of Expertise is from 3.67 to 3.79, and the value of Operations ranges from 4.11 to 4.14.

Security values for employees with 1 to 2 years, 2 to 3 years, 3 to 4 years, and more than 7 years of tenure are in the same order and are also fairly close. Where the value of Complexity is between 3.15 and 3.5, the value of Resilience is between 3.53 and 3.61, the value of Failure is from 3.6 to 3.78, the value of Expertise is from 3.71 to 3.91, and the value of Operations is between 3.98 and 4.13.

It is interesting to note how the security values change and their order for employees with 4 to 5 years of service and 5 to 6 years of service. The security value of Failure received the lowest scores among all other security values for employees with 4 to 5 years of tenure, indicating that the corresponding behavior is much less common for them than behaviors connected with other security values. The value of Complexity is the highest among all the employees with other tenure, with a score of 3.59, this demonstrates that they are trying to simplify as little as possible and are trying to covet data and evidence about their security environment when feasible. The value of Operations received the highest score of 4.28 for employees with 4 to 5 years of tenures and this shows a greater awareness of how things work in a security environment and ability to identify operational errors. For employees with 5 to 6 years of tenure is interesting to note correlation between security value of Complexity with the lowest score of 3.05 and the lowest score of 3.7 for security value of Operations. This reveals that oversimplification of the information security environment results in a failure to recognize errors that can lead to security breaches and possibly delays in incident response. Furthermore, the lowest score of 3.25 for the security value of Resilience implies that these employees are prone to loss track of the failure process and enter panic mode in the event of a crisis..

4.7 FORCE Value Metrics

The value metrics are concluded on the basis that a set of behaviors would achieve if they are all utilized together in Pipedrive. By monitoring these measurements, a company focused on reliability obtains an additional set of findings to compare to existing regulations and survey results.
Next, the author analyzes the resulting metrics to see how they compare with the FORCE Survey scores. It is worth noting that not all value metrics have been gathered since some of them are not yet measured at all. A complete table with FORCE Value Metrics results can be found in Appendix 4.

Security Value of Failure:

1. **Number of security failure scenarios developed in the past year**, answer: 8 and the corresponding survey score is 2.23. These results show that majority of employees are unfamiliar with existing failure scenarios and lack the expertise to anticipate any warning indicators in the failure cycle. This means that the eight failure scenarios prepared last year failed to fulfill their goals.

2. **Number of secuiry failures (whenever or not resulting in a formal security incident) reported in the past year**, answer: 18 incidents (scenarios not reported as incidents are not traceable) and the corresponding survey score is 2.79. This indicates that the accuracy of failure prediction activities has its drawbacks, and the existing identifiable failure markers are insufficient.

3. **Ratio of security incidents with no prior failure reporting or indicators in the past year**, answer: 18 and the corresponding survey score is 4.20. This demonstrates a reasonable level of comfort in reporting security problems up the chain of command. All minor event-related failures should be noticed before incidents occur and correlated with the corresponding failure scenarios, so the lower the ratio, the better the organization is at detecting small failures and managing incidents before the scenario fully escalates.

4. **Ratio of security failure or incident data (reports, root-cause analyses, after-actions, etc.) voluntarily shared outside the information security program**, answer: 0 (zero) and the corresponding survey score is 4.35. This

shows that even though information about security failures is not shared with those not responsible for security, most employees believe in the value and importance of sharing information about security problems.

5. **Ratio of security failures resulting in system changes**, answer: 7 and the corresponding survey score is 4.17. This means that many security incidents result in modifications to systems and lessons learned. However, it is better if minor failures are not ignored, and the necessary changes to the system are made immediately, before big problems accumulate in order to change the system.

Security Value of Operations:

1. **Level of security staff coverage for the organization (size of program, breadth of responsobility, systems managed, etc.),** answer: security program consists of 21 people, who are responsible for the entire Pipedrive and CRM application, the corresponding survey score is 4.39. This demonstrates the level of confidence most employees have in Pipedrive's security and shows the effectiveness of the information security structure.

2. **Number of security operations reviews completed in the past year**, answer: Internal Audit: no data; External Audit: once a year; GAP Assessment for SOC: once a year; the corresponding survey score is 4.08. This shows general reviews of InfoSec's operational performance and indicates that the majority of employees believe that Pipedrive has good information security management.

3. **Ratio of formally documented security operations or processes**, answer; no data; the corresponding survey score is 4.38. This demonstrates that most of employees feel that there are many experts at Pipedrive who are always willing to assist. However, there is no information on documented security processes or operations, indicating potential blind spots, unanticipated failures and lack of visibility in the security program.

4. **Ratio of security operational assessments shared outside the security group**, answer: external audit, once a year; the corresponding survey score is 3.90. This reveals that the InfoSec program is restricting the sharing of information about

operational security activities with outsiders, and this results in a lack of feedback from stakeholders in Pipedrive.

5. **Average time to address operational instabilities**, answer: 357 minutes, the corresponding survey score is 3.84. This indicates that there are adequate resources to address operational instability. Nonetheless, this value metric is a very useful indicator for estimating how long this process takes and a sign for improving visibility and problem solving.

Security Value of Resilience:

1. **Number of security-related training opportunities provided to people, by role or group, in the past year**, answer: Rangeforce learning platform is provided to all security roles; Rangeforce learning is also available for Engineers and General awareness training is done once a year to all roles in Pipedrive via KnowBe4; the corresponding survey score is 3.63. This demonstrates that most employees feel they are being trained to learn more about security than is required, however having skilled non-security professionals can help Pipedrive become more resilient.
2. **Number of identified security backup resources available during an incident**, answer: the specific number is not defined, but there is a mechanism for this called Security Guild. The most active members of this group can be backup resources. In addition, there are several security specialists in the Engineering department who may be backup, but the specific number has not been identified. The corresponding survey score is 4.06. This means that there are information security skills present in different departments, and in case of crises, these people can be highly valuable, but it is important to formally identify them in order to be able to contact them faster in case of a failure, to be able to better respond and recover from an incident.
3. **Ration of employees with identified security "challenge" assignments as part of regular performance reviews**, answer: 0 (zero), the corresponding survey score 3.53. This indicates that there are no requirements to participate in security challenges, however security challenge assignments should be offered, promoted, and rewarded to all who take part.

4. **Number and type of security knowledge sharing opportunities created in the past year**, answer: 1 - Online learning system; 2 - Security Guild; the corresponding survey score is 3.48. This emphasizes the importance of collaborating with other departments to improve information security understanding. Security teaching and knowledge sharing should be encouraged, and the outcomes should be evaluated.
5. **Number of scenario-based response testing or security war-game exercises conducted in the past year**, answer: 1; the corresponding survey score is 3.39. This metric shows limited failure scenarios and the necessity to conduct drills to see how employees respond to security events.

Security Value of Complexity:

1. **Number, type, and complexity of adopted organizational frameworks**, answer: ISO 27001, SOC 2; the corresponding survey score is 2.70. This shows that Pipedrive has several security frameworks that are used to manage information security. These are not simple models, however most people at Pipedrive prefer minimal complexity.
2. **Average time to organizational decisions (from initial proposal, through debate or deliberation, to final resolution),** answer: no data; the corresponding survey score is 3.69. Pipedrive does not measure such a metric, so there is no indicator of how fast and rigorous the decision-making process is. However, judging by the scores, the majority of employees are not ready to challenge or question the conclusions they have drawn.
3. **Average number of data points collected in support of individual organizational decisions**, answer: 3; the corresponding survey score is 3.65. This indicates that the number of data points obtained is limited, meaning that the benefit of complexity is unlikely to be effectively utilized or exploited.
4. **Number of formal reviews of security plans by non-security stakeholders in the past year**, answer: once a year; the corresponding survey score is 3.45. This metric shows that last year the cybersecurity program was subject to limited review, and people outside the security team hardly participated in discussions about security plans.

5. **Number of outcome and modeling evaluations conducted in the past year**, answer: 0 (zero), the corresponding survey score is 3.64. This demonstrates that there was no regular evaluation or revision of existing frameworks in the past year, and only a small percentage of Pipedrive's strategy and forecasts were reviewed to ensure accuracy and make improvements.

Security Value of Expertise:

1. **Number of formal knowledge or skill repositories in place**, answer: 1; the corresponding survey score 3.87. This shows that Pipedrive has a knowledge base, and most employees know where to find an expert if needed.
2. **Number of people with security responsobilities written into their job descriptions**, answer: 21 people; the corresponding score is 3.74. This means that security responsibilities do not extend beyond the information security department, but as Pipedrive grows and matures, security responsibilities should become universal in all job functions.
3. **Number of identified "quick response" scenarious with expedited decision making**, answer: no data; the corresponding survey score is 3.27. Pipedrive does not currently have "quick response" scenarios, so there is no pre-established quick chain of authority and pre-defined coordination.
4. **Number of decision owners for security formally assigned in the past year**, answer: ICS (Integrated Coaching Solution) with C-Suite; the corresponding survey score is 4.19. This demonstrates that there is defined authority to respond to a security situation.
5. **Number of cross-functional security-related activities or projects in the past year (initiated internally by the information security program or externally by other stakeholders),** answer: Security Guild - every other week, Weekly meetings with Infrastructure about vulnerabilities, Weekly engineering meetings, Disaster recovery exercise yearly; the corresponding survey score is 3.67. This metric demonstrates the current exchange and coordination of expert activities, however, there are not enough cross-functional security projects between all departments.

4.8 Connection between FORCE and Security Culture

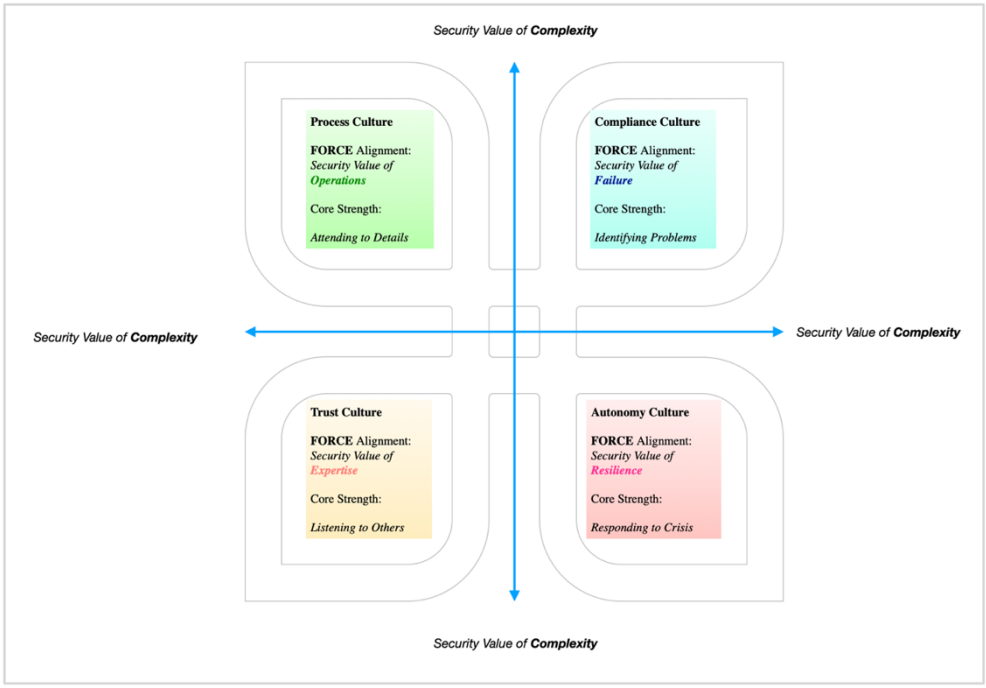

Figure 19. Security FORCE aligned to Security Cultures [2]

The alignment between Security Values and Security Culture, proposed by Hayden Lance [2] can be used to further understand how to implement a people-centric culture. The Security Culture assessment shows that the Trust Security Culture is dominant at Pipedrive, where a sense of community, trust and shared responsibility are important to employees. However, it is very important to recognize that the Trust Security Culture can only be successful if everyone in Pipedrive is a stakeholder in security and has the necessary knowledge, awareness and expertise. This requires all the departments to interact, collaborate and, importantly, communicate so that people understand what, why and how they should be doing. The Trust Culture is correlated with the Security Value of Expertise, as shown in Figure 19 and the evaluation of the Security FORCE values indicate that the Security Value of Expertise has a score of 3.75, which is below the desired level, as discussed earlier. Therefore, in order to thrive in the Trust Security Culture, it is important to start improving those key value behaviours related to a Security Value of Expertise and incorporate relevant metrics into Pipedrive's awareness program.

5 Proposed Guidelines

The author proposes the following guidelines based on the analysis of the collected data.

Desired Security Culture

Based on the analyzes, the dominant security culture is the Trust Security Culture, and it leads by a huge margin over all other cultures. However, only if everyone in Pipedrive is a stakeholder in security and has the essential knowledge, awareness, and experience can the Trust Security Culture succeed. Over the past few years, Pipedrive has grown rapidly in terms of the number of employees and the services they provide, and this year has reached a major milestone with over 100,000 companies now using the Pipedrive CRM platform. Pipedrive also has big plans for growth and development and is committed to launching a range of new native integrations relevant to small businesses with the goal of turning CRM into a revenue platform that connects all the tools needed for growth [31]. With continued growth, it is critical to have an equitable set of security values, where Trust Culture could be improved through awareness solutions to support everyone be a stakeholder in security, and also increasing levels of Process Security Culture by up to 25% and Compliance Security Culture by up to 25% to gain more insight and enable ongoing measurement.

The following methods are proposed by the author to assist in Security Culture transformation.

Leadership Awareness

Recognizing the need for a strong security culture starts from the top down and includes all members and all departments in Pipedrive. It is essential to have leadership that is prepared to foster a strong security culture, therefore top-level executives, as well as top-management have to participate in various workshops and awareness trainings to increase their understanding on the importance of developing strong security culture. Security certification programs should be available to leadership positions as well, and Pipedrive should support them with rewards and compensations. To ensure that management attends as much security training as possible, a variety of incentive strategies might be developed. Top executives must act as role models for CSC and take the initiative.

Security Awareness for Everyone

Cybersecurity training should be tailored to specific departments and should be related to their job responsibilities. For example, three training groups may be established, where Group 1 containing departments with a lack of IT skills, such as Customer Success, Finance, etc, Group 2 including Engineering departments and Group 3 having departments related to Information Security. As a result, all Pipedrive members will be more motivated to engage in training since it corresponds to their IT knowledge and will not be opposed by higher levels of training that should be available, to engineering departments, for example. The opposite is also true.

All members must participate in security trainings at regular intervals, intervals to be determined depending on the programs, and then re-take it to make sure their knowledge is up to date. The success or failure of training programs should be determined by measuring the effectiveness of information security training and comparing results over time.

In addition to trainings and exercises, on-going awareness program must be held within the Pipedrive to maintain a strong security culture. Games, events, posters, brochures, monthly newspaper articles, and internal badges for employees who performed security training can all be utilized to increase awareness. Another interesting option would be to develop a supplemental security awareness program for employee families to help their children and spouses become familiar with phishing, social engineering, and other security topics. A program like this could help foster a strong security culture among the Pipedrive community.

Cybersecurity Policy

The success of a cybersecurity culture depends on every person at Pipedrive. Awareness programs and training can help employees fully comprehend the ramifications of security incidents and how they may affect their day-to-day operations. However, people also must have up to date cybersecurity rules and policies to make sure they know where they fit and able to identify highly valued priorities of security program. The author proposes that all security stakeholders should participate in an annual review and update process to ensure that the standards and behaviors established in the cybersecurity policy are comprehensive.

SAT Plan

A clear plan should be created with outlined steps and timelines for all security training, awareness programs, attack simulations, seminars, games, tabletop exercises, rewards, and include tools to measure the effectiveness of the SAT.

Internal Bug Bounty Program

Many organizations offer bug bounty programs in which individuals can be rewarded for reporting bugs, particularly those relating to security risks. Pipedrive also established a private Bug Bounty Program for only invited hackers, which attracted over 300 participants. The total rewards paid out are over $300,000. It's a good program that aids in the detection of bugs before they harm customers and the prevention of widespread incidents. However, the author believes that most of the bugs and vulnerabilities could also be discovered by local teams in Pipedrive. There is some reporting mechanism for reporting bugs and failures, however this may only be available to engineering departments. Therefore, a similar mechanism should be established for all other departments and reporting should be as easy as possible. Such an activity should be backed up by recognition and compensation to urge all participants to actively engage. As a result, internal bug bounty program will be established, resulting in increased security awareness, and stronger security culture.

FORCE Boost

Because the Trust Security Culture and the Security Value of Expertise are naturally aligned, start with improving associated behavior will be very successful and will deliver immediate benefits. The following steps will help to rise the security value of expertise:

- Sharing Expertise, create skill repositories where anyone can add themselves and their skills.
- Create "quick response" scenarios with accelerated decision making to bypass bureaucracy.
- Initiate cross-functional security related activities involving people from all departments.

To improve the security value of failure the following steps have to be implemented:

- Encourage people to appreciate failures but be clear that not every failures are created equally and that learning from little mistakes can actually help avoid big disasters.
- The teams responsible for security have to be transparent about security failures and share this information with other departments to influence them to report the failures they encounter.
- Develop as many security failure scenarios as possible.
- To be able to foresee security issues, analyze and look for trends in reported bugs and failures.

To improve the security value of resilience the following steps have to be implemented:

- Identify a group of people outside of InfoSec who can serve as a backup resource in the event of an incident.
- Conduct security war-game exercises for all departments to test how well is respond and practice failing.
- Improve on online learning systems and sharing knowledge base.
- Create a shadowing program, where people from other departments can shadow a member of a InfoSec for a day. It is also, good to have shadowing in other departments to gain a deeper understanding of processes and functions.

Stress Management Program

- Exercise teamwork regularly in stressful threat scenarios. A set of detection and mitigation techniques must also be designed and practiced ahead of time. Teams should not improvise in moments of crisis, when stress and anxiety are high, and the clock is approaching potential disaster. When time is limited, bringing a group of individuals together and expecting them to figure out how to work together as a team will not work.
- Increase team diversity in terms of experience and culture in order to maximize threat detection.
- In order to combat psychological factors that silence ambiguous threats, systems must be devised for magnifying warning indicators, even if they appear innocuous at first.
- Creation an environment with psychological safety, where everyone is encouraged to share their concerns.

6 Future Steps and Limitations

The study met its objectives, although there are a few limitations that will require more research to complement and strengthen the current findings.

Limitations

Due to time constrains, the author had to conduct two surveys with a very short time interval. Some employees got confused between the two surveys and may not have taken part in the second survey because they thought it was still the first survey. For best results, the time between assessments should be at least three months.

Due to time constraints, the survey evaluation time was three weeks for the first survey and two weeks for the second survey. It would also be more beneficial if each survey could be accessed for four weeks in order to get the maximum number of responses.

Although the author only conducted a quantitative study, other methodologies, such as qualitative research through interviews, may be able to provide useful information about the proposed guidelines.

Future Research

Qualitative research through interviews and feedback can be added to complement future research.

The second round of the Security Culture survey and the FORCE survey should preferably be repeated in Pipedrive in about a year. The results of the surveys completed as part of this research should serve as a baseline against which the second assessment can be compared. Thus, the proposed guidelines developed as a result of this security culture research and implemented will be evaluated and the positive transformation of security culture can be seen.

Additional cyber security culture research can be carried out in various business areas, for example, it can be done in all unicorn companies in Estonia. The data can be compared to assess how strong security culture is in Estonian business and which security culture is most prevalent.

7 Conclusion

The goal of this thesis was to develop a collection of guidelines and best practices that Cyber Security specialists, IT professionals and businesses across all industries can utilize to ensure consistent improvement in a people-centric security culture. The author focused on diagnosing different cultures, addressing specific behaviours and the importance of developing transformation strategies towards a strong security culture in Pipedrive. The author used a quantitative method to collect data about existing security culture and associated key value behaviours. The analysis of gathered data revealed that the highest scores were given to the Trust Security Culture, which is around 37.3% from all other cultures, which means that team collaboration and shared responsibility are highly valued and prioritized in Pipedrive. Despite the fact that Information Security and IT Ops departments have the lowest scores for trust culture responses, nevertheless, based on the percentage distribution across cultures, trust culture still scores highest. This indicates that Pipedrive's security experts do not view humans as threat actors, but rather strive to provide them with the greatest tools to make the best security decisions possible. The results of the survey on key security values revealed that the highest scores were given to the Security Value of Operations, with an average of 4.12, which demonstrates that employees in Pipedrive understand how overall things work in a security environment and that there are systems in place for identifying errors that could lead to failures. The lowest scores were given to Security Value of Complexity, indicating that there is an oversimplification that creates unnecessary risk and overlooks the importance of hidden aspects that could potentially destabilize the ability to respond to threats. Another finding emphasizes the significance of enhancing key value behaviours associated with the Security Value of Expertise, which is linked to the Security Trust Culture and therefore should have higher scores than at the moment in order for the Trust Culture to thrive.

The results of this research should serve as a baseline for the second assessment, which may be carried out approximately one year after the implementation of all developed guidelines. In the future, it would be useful to conduct additional research in various areas of business in order to verify the validity of these findings in other types of businesses with different security cultures.

This research shows that using the guidelines proposed by the author, such as developing a balanced, people-centric security culture, recognizing the need for a leadership security awareness program, as well as specific security training for everyone, including family members, improving cybersecurity policy and creating an internal bug bounty program, implementing FORCE Boost and a dedicated cybersecurity stress management program can ensure the maximum success in building the best people-centric cybersecurity culture.

References

[1] "KnowBe4. Security Culture Report," [Online]. Available: https://www.knowbe4.com/organizational-cyber-security-culture-research-report. [Accessed 18 04 2022].

[2] L. Hayden, People-centric security: transforming your enterprise security culture., McGraw Hill Professional, 2015.

[3] "enisa.europa.eu Cyber Security Culture in organisations," November 2017. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport. [Accessed 17 April 2022].

[4] J. D. Nosworthy, "Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?," *Computers & Security,* vol. 19, no. 4, pp. 337-347, 2000.

[5] I. I. Tuija Kuusisto, "nformation security culture in small and medium size enterprises," *Frontiers of e-business Research,* 2003.

[6] A. d. Veiga, *Cultivating and Assessing Information Security Culture,* University of Pretoria, 2008.

[7] N. M. Adéleda Veiga, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security,* vol. 49, no. March, pp. 162-176, 2015.

[8] The 2002 Security Guidelines , "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," *OECD,* no. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2002.

[9] S. Dojkovski, S. Lichtenstein and M. J. and Warren, "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia," in *ECIS 2007 Proceedings.120*, 2007.

[10] R. v. S. Johan van Niekerk, "UNDERSTANDING INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK," in *Centre for Information Security Studies,*, Nelson Mandela Metropolitan University, South Africa, 2006.

[11] A. &. E. J. Martins, "Information security culture," in *IFIP Advances in Information and Communication Technology*, IFIPAICT, 2002.

[12] S. T. Thomas Schlienger, "INFORMATION SECURITY CULTURE – FROM ANALYSIS TO CHANGE," University of Fribourg, 2005.

[13] "Coveware: Ransomware Recovery First Responders.," [Online]. Available: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020. [Accessed 18 April 2022].

[14] W. Z. S. B. A. S. Xin (Robert) Luo, "Investigating phishing victimization with the HeuristiceSystematic Model: A theoretical framework and an exploration," *Computers & Security,* vol. 38, no. October, pp. 28-38, 2013.

[15] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," Benchmark research sponsored by Symantec, 2013.

[16] S. v. S. M.M Eloff, "Information Security Management: An Approach to Combine Process Certification And Product Evaluation," *Computers & Security,* vol. 19, no. 8, pp. 698-709, 2000.

[17] P. K. R. Anita-Catrin Eriksen Gregor Petrič, "Security Culture and Credential Sharing," https://www.knowbe4.com/hubfs/Security%20Culture%20and%20Credential%20Sharing.pdf, 2021.

[18] Osterman Research, "Survey Report by Osterman Research, 2020, Security Awareness Training as a Key Element in Changing the Security Culture," https://ostermanresearch.com/2022/03/29/orwp_0352/, 2020.

[19] C. Cimpanu, "Ryuk Ransomware Crew Makes $640,000 in Recent Activity Surge," 21 August 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/ryuk-ransomware-crew-makes-640-000-in-recent-activity-surge/. [Accessed 24 April 2022].

[20] J. Henry, "9 Reasons Why Cybersecurity Stress Is an Industry Epidemic," Security Intelligence , 14 January 2020. [Online]. Available: https://securityintelligence.com/articles/9-reasons-why-cybersecurity-stress-is-an-industry-epidemic/]. [Accessed 24 April 2022].

[21] "Navigating the Digital Age, Third Edition, the Definitive Guide for Directors and Officers.," 15 October 2015. [Online]. Available:

https://www.securityroundtable.org/navigating-the-digital-age-3rd-edition/. [Accessed 20 April 2022].

[22] C. Duhigg, "What Google learned from its quest to build the perfect team," *The New York Times Magazine,* 2016.

[23] "The Representativeness Heuristic," [Online]. Available: https://thedecisionlab.com/biases/representativeness-heuristic. [Accessed 24 April 2022].

[24] "Cambridge Dictionary," [Online]. Available: https://dictionary.cambridge.org/dictionary/english/confirmation-bias. [Accessed 20 April 2022].

[25] "Cognitive Consistency (SOCIAL PSYCHOLOGY)," ResearchNet., [Online]. Available: https://psychology.iresearchnet.com/social-psychology/attitudes/cognitive-consistency/. [Accessed 24 April 2022].

[26] E. b. D. C. a. A. Zander, Group Dynamics: Research and Theory. Third Edition., London: Tavistock Publications, 1968.

[27] R. M. B. a. A. C. E. Michael Roberto, " Facing Ambiguous Threats," Harvard Business Review, November 2006. [Online]. Available: https://hbr.org/2006/11/facing-ambiguous-threats. [Accessed 24 April 2022].

[28] J. Cano, R. Hernandez, R. Pastor, S. Ros, L. Tobarra and A. Robles-Gomez, "Developing Metacognitive Skills for Training on Information Security," in *Online Engineering & Internet of Things*, 2018, pp. 708-720.

[29] M. L. t. P. C. Stefano De Dominicis, "Metacognitive Therapy for Work-Related Stress: A Feasibility Study," *Front. Psychiatry,* 2021.

[30] "Pipedrive," Pipedrive, [Online]. Available: https://www.pipedrive.com/en/jobs. [Accessed 24 April 2022].

[31] Pipedrive, "Pipedrive reaches 100K customer milestone initiating a new growth phase" Pipedrive, 22 February 2022. [Online]. Available: https://www.pipedrive.com/en/newsroom/pipedrive-reaches-100k-customer-milestone-initiating-a-new-growth-phase. [Accessed 24 April 2022].

Appendix 1 - Thesis Security Culture Survey Questions

The following are the questions and answer options developed by Lance Hayden [2] and used by the author to gather the necessary data for the thesis:

Q1		**What's valued most in Pipedrive?**
	A	**Stability and reliability** are valued most in Pipedrive. It is critical that everyone knows the rules and follows them. We cannot succeed if people are all doing things different ways without centralized visibility.
	B	**Successfully meeting external requirements** is valued most in Pipedrive. We are under a lot of scrutiny. We cannot succeed if people fail audits or do not live up to the expectations of those watching.
	C	**Adapting quickly and competing aggressively** are valued most in Pipedrive. Results are what matters. We cannot succeed if bureaucracy and red tape impair people's ability to be agile.
	D	**People and a sense of community** are valued most in Pipedrive. Everyone is in it together. We cannot succeed unless people are given the opportunities and skills to succeed on their own.
Q2		**How does Pipedrive generally work?**
	A	Pipedrive works on **authority, policy, and standard ways of doing things**. Organizational charts are formal and important. The organization is designed to ensure control and efficiency.
	B	Pipedrive works on **outside requirements and regular reviews**. Audits are a central feature of life. The organization is designed to ensure everyone meets their obligations.
	C	Pipedrive works on **independent action and giving people decision authority**. There's no one right way to do things. The organization is designed to ensure that the right things get done in the right situations.
	D	Pipedrive works on **teamwork and cooperation**. It is a community. The organization is designed to ensure everyone is constantly learning, growing, and supporting one another.
Q3		**What does 'security' mean in Pipedrive?**
	A	Security means **policies, procedures, and standards, automated wherever possible using technology.** When people talk about security they are talking about the infrastructures in place to protect Pipedrive's information assets.
	B	Security means **showing evidence of visibility and control, particularly to external parties**. When people talk about security they are talking about passing an audit or meeting a regulatory requirement.
	C	Security means **enabling the organization to adapt and compete,** not hindering it or saying "no" to everything. When people talk about security they are talking about balancing risks and rewards.
	D	Security means **awareness and shared responsibility**. When people talk about security they are talking about the need for everyone to be an active participant in protecting the organization.
Q4		**How is information managed and controlled in Pipedrive?**
	A	Information is seen as a **direct source of business value,** accounted for, managed, and controlled like any other business asset. Formal rules and policies govern information use and control.
	B	Information is seen as a **sensitive and protected resource,** entrusted to the organization by others and subject to review and audit. Information use and control must always be documented and verified.
	C	Information is seen as a **flexible tool that is the key to agility and adaptability** in the organization's environment. Information must be available where and when it is needed by the business, with a minimum of restrictive control.
	D	Information is seen as **the key to people's productivity, collaboration, and success**. Information must be a shared resource, minimally restricted, and available throughout the community to empower people and make them more successful.
Q5		**How are operations generally managed in Pipedrive?**
	A	Operations are **controlled and predictable**, managed according to the same standards throughout the organization.
	B	Operations are **visible and verifiable**, managed and documented in order to support audits and outside reviews.
	C	Operations are **agile and adaptable**, managed with minimal bureaucracy and capable of fast adaptation and flexible execution to respond to changes in the environment.

	D	Operations are **inclusive and supportive**, allowing people to master new skills and responsibilities and to grow within the organization.
Q6		**How is technology managed in Pipedrive?**
	A	Technology is **centrally managed**. Standards and formal policies exist to ensure uniform performance internally.
	B	Technology is **regularly reviewed**. Audits and evaluations exist to ensure the organization meets its obligations to others.
	C	Technology is **locally managed**. Freedom exists to ensure innovation, adaptation, and results.
	D	Technology is **accessible to everyone.** Training and support exists to empower users and maximize productivity.
Q7		**How are people managed in Pipedrive?**
	A	People must **conform to the needs of the organization**. They must adhere to policies and standards of behavior. The success of the organization is built on everyone following the rules.
	B	People must **demonstrate that they are doing things correctly**. They must ensure the organization meets its obligations. The success of the organization is built on everyone regularly proving that they are doing things properly.
	C	People must **take risks and make quick decisions**. They must not wait for someone else to tell them what's best. The success of the organization is built on everyone experimenting and innovating in the face of change.
	D	People must **work as a team and support one other.** They must know that everyone is doing their part. The success of the organization is built on everyone learning and growing together.
Q8		**How is risk managed in Pipedrive?**
	A	Risk is managed **by getting rid of deviations in the way things are done.** Increased visibility and control reduce uncertainty and negative outcomes. The point is to create a reliable standard.
	B	Risk is managed **by documentation and regular review.** Frameworks and evaluations reduce uncertainty and negative outcomes. The point is to keep everyone on their toes.
	C	Risk is managed **by decentralizing authority.** Negative outcomes are always balanced by potential opportunities. The point is to let those closest to the decision make the call.
	D	Risk is managed **by sharing information and knowledge.** Education and support reduce uncertainty and negative outcomes. The point is to foster a sense of shared responsibility.
Q9		**How is accountability achieved in Pipedrive?**
	A	Accountability is **stable and formalized.** People know what to expect and what is expected of them. The same rewards and consequences are found throughout the organization.
	B	Accountability is **enabled through review and audit.** People know that they will be asked to justify their actions. Rewards and consequences are contingent upon external expectations and judgments.
	C	Accountability is **results-driven.** People know there are no excuses for failing. Rewards and consequences are a product of successful execution on the organization's business.
	D	Accountability is **shared among the group.** People know there are no rockstars or scapegoats. Rewards and consequences apply to everyone because everyone is a stakeholder in the organization.
Q10		**How is performance evaluated in Pipedrive?**
	A	Performance is evaluated **against formal strategies and goals.** Success criteria are unambiguous.
	B	Performance is evaluated **against the organization's ability to meet external requirements.** Audits define success.
	C	Performance is evaluated **on the basis of specific decisions and outcomes.** Business success is the primary criteria.
	D	Performance is evaluated **by the organizational community.** Success is defined through shared values, commitment, and mutual respect.

Appendix 2 - Thesis FORCE Survey Statements

The following are the FORCE statements developed by Lance Hayden [2] and used by the author to gather the necessary data for the thesis:

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Security Value of Failure					
1. I feel confident I could predict where the organization's next security incident will happen.					
2. I regularly identify security problems while doing my job.					
3. I feel very comfortable reporting security problems up the management chain.					
4. I know that security problems I report will be taken seriously.					
5. When a security problem is found, it gets fixed.					
Security Value of Operations					
1. I know that someone is constantly keeping watch over how secure the organization is.					
2. I am confident that information security in the organization actually works the way that people and policies say it does.					
3. I feel like there are many experts around the organization willing and able to help me understand how things work.					
4. Management and the security team regularly share information about security assessments.					
5. Management stays actively involved in security and makes sure appropriate resources are available.					
Security Value of Resilience					
1. I feel like people are trained to know more about security than just minimum level necessary.					
2. The organization has reserves of skill and expertise to call on in the event of a security incident or crisis.					
3. I fell like everyone in the organization is encouraged to "get out of their comfort zone" and be part of security challenges.					
4. I feel like people are interested in what I know about security, and willing to share their own skills to help me as well.					
5. The organization often conducts drills and scenarios to test how well we respond to security incidents and failures.					
Security Value of Complexity					
1. I feel like people in the organization prefer complex explanations over simple ones.					
2. I feel like people are open to being challenged or questioned about how they arrived at an answer.					
3. The organization always has plenty of data to explain and justify its decisions.					
4. People from outside the security team are encouraged to participate and question security plans and decisions.					
5. The organization formally reviews strategies and predictions to make sure they were accurate, and adjusts accordingly.					
Security Value of Expertise					
1. I know exactly where to go in the organization when I need an expert.					

2. I think everyone in the organization feels that monitoring security is part of their job.					
3. In the event of a security incident, people can legitimately bypass the bureaucracy to get things done.					
4. People in the organization are encouraged to help other groups if they have the right skills to help them.					
5. I feel empowered to take action myself, if something is about to cause a security failure.					

Appendix 3 - FORCE mapped with Metrics & Key Value Behaviors

The following statements, key behaviors and metrics developed by Lance Hayden [2] and used by the author to analyze necessary data for the thesis:

FORCE SURVEY Statements	Key Value Behaviours	FORCE Metrics
Security Value of Failure		**Security Value of Failure**
1. I feel confident I could predict where the organization's next security incident will happen.	• Anticipate failures	1. Number of security failure scenarious developed in the past year
2. I regularly identify security problems while doing my job.	• Seek out problems	2. Number of secuiry failures (whenever or not resulting in a formal security incident) reported in the past year.
3. I feel very comfortable reporting security problems up the management chain.	• Reward problem reporting	3. Ratio of security incidents with no prior failure reporting or indicators in the past year
4. I know that security problems I report will be taken seriously.	• Share information about failure	4. Ratio of security failure or incident data (reports, root-cause analyses, after-actions, etc.) voluntarily shared outside the information security program
5. When a security problem is found, it gets fixed.	• Learn from mistakes	5. Ratio of security failures resulting in system changes
Security Value of Operations		**Security Value of Operations**
1. I know that someone is constantly keeping watch over how secure the organization is.	• Keep your eyes open	1. Level of security staff coverage for the organization (size of program, breadth of responsobility, systems managed, etc.)
2. I am confident that information security in the organization actually works the way that people and policies say it does.	• Form a bigger picture	2. Number of security operations reviews completed in the past year
3. I feel like there are many experts around the organization willing and able to help me understand how things work.	• “Listen” to the system	3. Ratio of formally documented security operations or processes
4. Management and the security team regularly share information about security assessments.	• Test expectations against reality	4. Ratio of security operational assessments shared outside the security group
5. Management stays actively involved in security and makes sure appropriate resources are available.	• Share operational assessments	5. Average time to address operational instabilities
Security Value of Resilience		**Security Value of Resilience**
1. I feel like people are trained to know more about security than just minimum level necessary.	• Overtrain people	1. Number of security-related training opportunities provided to people, by role or group, in the past year
2. The organization has reserves of skill and expertise to call on in the event of a security incident or crisis.	• Create “Skill benches”	2. Number of identified security backup resources available during an incident
3. I fell like everyone in the organization is encouraged to "get out of their comfort zone" and be part of security challenges.	• Actively share expertise	3. Ration of employees with identified security "challenge" assignments as part of regular performance reviews

4. I feel like people are intersted in what I know about security, and willing to share their own skills to help me as well.	• Encourage stretch goals	4. Number and type of security knowledge sharing opportunities created in the past year
5. The organization often conducts drills and scenarious to test how well we respond to security incidents and failures.	• Practice failing	5. Number of scenario-based response testing or security war-game exercises conducted in the past year
Security Value of Complexity		**Security Value of Complexity**
1. I feel like people in the organization prefer complex explanations over simple ones.	• Don’t oversimplify	1. Number, type, and complexity of adopted organizational frameworks
2. I feel like people are open to being challenged or questioned about how they arrived at an answer.	• Formalize your assumptions	2. Average time to organizational decisions (from initial proposal, through debate or deliberation, to final resolution)
3. The organization always has plenty of data to explain and justify its decisions.	• Covet empirical evidence	3. Average number of data points collected in support of individual organizational decisions
4. People from outside the security team are encouraged to participate and question security plans and decisions.	• Share the doubt	4. Number of formal reviews of security plans by non-security stakeholders in the past year
5. The organization formally reviews strategies and predictions to make sure they were accurate, and adjusts accordingly.	• Make every model better	5. Number of outcome and modeling evaluations conducted in the past year
Security Value of Expertise		**Security Value of Expertise**
1. I know exaclty where to go in the organization when I need an expert.	• Ask the experts	1. Number of formal knowledge or skill repositories in place
2. I think everyone in the organization feels that monitoring security is part of their job.	• Suppress the ego	2. Number of people with security responsobilities written into their job descriptions
3. In the event of a security incident, people can legitimately bypass the bureaucracy to get things done.	• Allow authority to migrate	3. Number of identified "quick response" scenarious with expedited decision making
4. People in the organization are encouraged to help other groups if they have the right skills to help them.	• Share credibility	4. Number of decision owners for security formally assigned in the past year
5. I feel empowered to take action myself, if something is about to cause a security failure.	• Reward calls to action and cries for help	5. Number of cross-functional security-related activities or projects in the past year (initiated internally by the information security program or externally by other stakeholders)

Appendix 4 – Security Culture and FORCE Survey Results

Due to the very large size of the results tables, results are available at the following links:

https://gitlab.cs.ttu.ee/nasemj/security-culture-survey-results

https://github.com/Nadezda123/Security-Culture-Survey-Results

Appendix 5 – FORCE Metrics Results

The following are the Metrics parameters developed by Lance Hayden [2] and the results obtained by the author in Pipedrive for the purposes of this thesis:

FORCE METRICS	METRICS RESULTS	FORCE SCORE
Security Value of Failure		
1. Number of security failure scenarious developed in the past year	8	2.23
2. Number of secuiry failures (whenever or not resulting in a formal security incident) reported in the past year.	18 incidents (scenarios not reported as incidents are not traceable)	2.79
3. Ratio of security incidents with no prior failure reporting or indicators in the past year	18	4.20
4. Ratio of security failure or incident data (reports, root-cause analyses, after-actions, etc.) voluntarily shared outside the information security program	0	4.35
5. Ratio of security failures resulting in system changes	7	4.17
Security Value of Operations		
1. Level of security staff coverage for the organization (size of program, breadth of responsobility, systems managed, etc.)	Program consists of 21 people. Coverage is the entire organisation and the Pipedrive CRM application.	4.39
2. Number of security operations reviews completed in the past year	Internal Audit: N/A; External Audit: once year; GAP Assessment for SOC: once a year	4.08
3. Ratio of formally documented security operations or processes	N/A	4.38
4. Ratio of security operational assessments shared outside the security group	External audit, once a year.	3.90
5. Average time to address operational instabilities	357	3.84
Security Value of Resilience		

1. Number of security-related training opportunities provided to people, by role or group, in the past year	Rangeforce learning platform is provided to all security roles. Rangeforce learning is also available for Engineers and General awareness training is done once a year to all roles in Pipedrive via KnowBe4	3.63
2. Number of identified security backup resources available during an incident	The number in specific has not been defined, but we have a mechanism for that and that is called Security Guild. The most active members from that group can be backup resources. In addition we have several security aware people across Engineering that are capable to be backup. But the specific number has not been identified.	4.06
3. Ration of employees with identified security "challenge" assignments as part of regular performance reviews	0	3.53
4. Number and type of security knowledge sharing opportunities created in the past year	1 - Online learning system, 2 - Security Guild	3.48
5. Number of scenario-based response testing or security war-game exercises conducted in the past year	1	3.39
Security Value of Complexity		
1. Number, type, and complexity of adopted organizational frameworks	ISO 27001, SOC 2	2.70
2. Average time to organizational decisions (from initial proposal, through debate or deliberation, to final resolution)	N/A	3.69
3. Average number of data points collected in support of individual organizational decisions	3	3.65
4. Number of formal reviews of security plans by non-security stakeholders in the past year	Once a year	3.45
5. Number of outcome and modeling evaluations conducted in the past year	0	3.64
Security Value of Expertise		
1. Number of formal knowledge or skill repositories in place	1	3.87

2. Number of people with security responsobilities written into their job descriptions	21	3.74
3. Number of identified "quick response" scenarious with expedited decision making	N/A	3.27
4. Number of decision owners for security formally assigned in the past year	ICS (Integrated Coaching Solution) with C-Suite	4.19
5. Number of cross-functional security-related activities or projects in the past year (initiated internally by the information security program or externally by other stakeholders)	Security Guild - every other week, Weekly meetings with Infrastructure about vulnerabilities, Weekly engineering meetings, Disaster recovery exercise yearly	3.67

Appendix 6 – Analysis of Business Intelligence Department

1. What's valued the most in Pipedrive?

Response "A" received the highest percentage of 30%, which means that Stability and Reliability are valued the most in this department, and they prefer to have centralized visibility and common rules.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 55%, which means that they work as a team and value cooperation. This department sees the benefits in constantly learning and supporting each other.

3. What does 'security' mean in Pipedrive?

The answer "D" received the highest percentage of 36.6%, which means that they view security as a shared responsibility and value being actively involved in creating security awareness.

4. How is information managed and controlled in Pipedrive?

Response "D" received the highest percentage of 42%, which means that information is considered as a key to productivity and success. Sharing information is highly valued as it empowers people and promotes collaboration.

5. How are operations generally managed in Pipedrive?

The answer "D" received the highest percentage of 47%, which means that the operating environment in this department is favorable and allows to learn new skills and support growth.

6. How is technology managed in Pipedrive?

Response "C" received the highest percentage of 50.5% and this is also the highest score 5.1 for this answer among all the departments. Which means that for Business Intelligence Department technology is managed locally and subject to less control. Freedom exists to ensure progress and results. It is interesting to point out that the lowest percentage 10.9% and score 1.1 received answer "B", where technology is regularly reviewed and regular audits and evaluations performed. This indicate that this department has no or limited obligations to others in terms of technology performance and does not conduct regular technology reviews.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 52.5%, which means that teamwork is an important part of the company's success, where everyone learns and grows together.

8. How is risk managed in Pipedrive?

Response "D" received the highest percentage of 40%, which means that in this department the risk is best managed through the exchange of information and knowledge, where a sense of shared responsibility for risk is nurtured.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 57%, indicating overall accountability in the team. Rewards and failures apply to all and equality in accountability is maintained. It is interesting to point out that the lowest percentage 8% and the score 0.8, the lowest among all departments was given to response “A”. Answer "A" means that accountability is stable and formalized and expectations are clear to people. Such a low score for this answer indicate that accountability in this department is perceived less mechanistically, and individual accountability is inferior to group accountability.

10. How performance evaluated in Pipedrive?

The answer "C" received the highest percentage of 47.5% and the highest score of 4.8 among all departments. The Business Intelligence Department considers business success as the main criterion for evaluating performance. Specific decisions and consequences are used to assess performance. Answer “B” received a score of 0.6, which is also the lowest score among all departments, which mean that external audit is not an important criterion for evaluating performance.

Appendix 7 - Analysis of Customer Success Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 42.6%, which is also close to the average percentage of 42.5% among all teams, which demonstrates that people and the feeling of family, where everyone shares responsibility together, are most valued in Pipedrive. The smallest percentage received a "B" answer and is below the average percentage of 16% for the same answer among all departments. This is an interesting result because this answer is in line with the Compliance Security Culture and indicate that external requirements and audits are the least valued in this Department. However, this team is constantly working with external parties, such as customers, and the level of these core values influences the security culture in such relationships.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 42.7%, which shows that they prefer teamwork and value cooperation. This department sees the benefits in human relationships, in supporting each other and sharing responsibility.

3. What does 'security' mean in Pipedrive?

The answer "D" received the highest percentage of 43%, which is 5% higher than the average percentage for this answer, this means that they perceive security as a shared responsibility and want to actively participate in raising security awareness. It is interesting to note that, during the survey, the author was only approached by people from this department who offered their support for the security culture transformation project and also offered to include the survey in their training plan that they provide regularly to employees.

4. How is information managed and controlled in Pipedrive?

Response "B" received the highest percentage of 34%, which is above by 4.3% the average percentage of 30% among all other departments, which reveals that information is treated as a confidential and protected resource. Because they are constantly working with clients and other external parties, the people in this department understand that Information must be verified, protected and documented as it is subject to verification and external audit.

5. How are operations generally managed in Pipedrive?

The answer "D" received the highest percentage of 33%, this shows that the day-to-day operations in this department are favorable and supportive, allowing employees to learn new skills and responsibilities that could lead to career advancement in Pipedrive.

6. How is technology managed in Pipedrive?

The answer "D" received the highest percentage of 35.1%, this indicates that the technology is perceived as an accessible tool for everyone. In this department, technology is used to improve the success of internal stakeholders and maximize productivity.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 47.7%, which means that teamwork is very important in this department, where people receive special support and development opportunities.

8. How is risk managed in Pipedrive?

The answer "D" received the highest percentage of 42.2%, this demostrates that in this department they believe that risk is best managed if everyone shares knowledge, experience and information.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 35.7%, which shows that people in this department share the accountability among each other. Everyone makes decisions and does their job on the assumption that rewards and consequences are shared among the team.

10. How performance evaluated in Pipedrive?

The answer "D" received the highest percentage of 38.3%, indicating that performance measurement is defined in terms of shared values and mutual respect, rather than who is responsible for those successes or failures.

Appendix 8 - Analysis of Finance Department

1 What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 38.8%, which is 3.7% lower than the overall average percentage of 42.5% among all departments, which means that people and a sense of community when everyone shares responsibility together is very important for them. Here it should be noted that the answer "B", associated with Autonomy Security Culture, received 29.1%, which is 8.3% higher than the average, which shows that this department also greatly values competitiveness and adaptation to the environment in order to achieve the highest results.

2. How does Pipedrive generally work?

The "D" answer received the highest percentage of 56.6%, which is 11.3% higher than the average percentage for this answer. This indicates that people in the Finance department see their work as a team effort, where the value is that everyone benefits from such cooperation and constantly supports each other in order to achieve common goals.

3. What does 'security' mean in Pipedrive?

The "D" answer received the highest percentage of 33.3%, which is 4.7% lower than the average percentage for this answer. This reveals that they perceive security as a shared responsibility in which everyone is an active participant, but also based on the high percentage of "A" responses, it is important for this team to have automated security infrastructure, security policies and procedures in place to protect information resources.

4. How is information managed and controlled in Pipedrive?

Answer "A" , associated with Process Security Culture, received the highest percentage of 35.6%, up 12.9% from the average percentage of 22.7% among all other departments. This is quite a big divergence from other departments in how information should be managed and controlled. Since this is a Finance department that deals with monetary tasks, it is understandable that they view information as a direct source of business value that needs to be accounted for and controlled. Policies and formal rules must exist to manage information.

5. How are operations generally managed in Pipedrive?

Answer "C" received the highest percentage of 36.3%, which is 8.5% higher than the average percentage for this answer. This demostrates that day-to-day functions should be

managed with less bureaucracy, and that decision-making and interactions should be flexible in order to respond to any changes in the shortest possible time.

6. How is technology managed in Pipedrive?

Answer "D" received the highest percentage of 50%, which is 18.5% higher than the average percentage for this answer. It's also the highest average score of 5.9 for this answer, which show big differences with other teams in how they see technology being managed. In this department, technological freedom is highly valued, where technology is available to everyone, and everyone should benefit from it in order to achieve maximum success.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 47.3%, which reveals that teamwork is very important in this department, where people know that they will receive any support and they have many opportunities for development.

8. How is risk managed in Pipedrive?

Answer "D" received the highest percentage of 59.5%, which is 20.8% higher than the average percentage for this answer. This is also the highest average score of 6.6 for this answer, which indicate big differences with other teams in how they view risk management. Finance department believes sharing information and knowledge is the best way to manage risk, or at least that's how they understand it is done in Pipedrive. This department sees great value in trainings and support in order to reduce the number of failures and negative consequences.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 46.8%, which means that people in this department value shared accountability. The rewards as well as the negative consequences are shared by everyone because everyone takes ownership and responsibility.

10. How performance evaluated in Pipedrive?

The answer "D" received the highest percentage of 34.6%, indicating that the performance is evaluated by the internal community. In the Finance department, success criteria are defined through shared values and mutual respect.

Appendix 9 – Analysis of G & A Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 45%, which is 2.5% higher than the overall average percentage of 42.5% among all departments. This indicates that a sense of family is very important to them. Human development and provided opportunities in the company are also highly valued.

2. How does Pipedrive generally work?

The "D" answer received the highest percentage of 44.3%, which is 1% lower than the average percentage for this answer. This shows that people in the Finance department see their work as a team effort, where the value is that everyone benefits from such cooperation and constantly supports each other in order to achieve common goals.

3. What does 'security' mean in Pipedrive?

The "D" answer received the highest percentage of 43.8%, which is 5.8% higher than the average percentage for this answer. This demonstrates that they perceive security as a shared responsibility in which everyone is an active participant. Important to note that the lowest percentage was given to "B" response, which is also the lowest among all the departments. This means that G&A is not subject to any external security audit or has limited requirements to external organizations to comply with any security regulations.

4. How is information managed and controlled in Pipedrive?

The "D" response associated with Trust Security Culture received the highest percentage of 30.9%, which is 2.7% higher than the average percentage among all other departments. This shows that the G&A department treats information as a shared resource, it is almost not restricted and is widely used to increase productivity and success in Pipedrive.

5. How are operations generally managed in Pipedrive?

Answer "D" received the highest percentage of 34.2%, which is 1.2% higher than the average percentage for this answer. This demonstrates that the day-to-day operations in this department are favorable and supportive, allowing employees to learn new skills and responsibilities that could lead to career advancement in Pipedrive.

6. How is technology managed in Pipedrive?

Answer "D" received the highest percentage of 36.2%, which is 4.7% higher than the average percentage for this answer. In this department, technological freedom is highly

valued, where technology is available to everyone, and everyone should benefit from it in order to achieve maximum productivity.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 60.2%, which is 13.8% higher than the average percentage for this answer. This shows that teamwork is highly valued and people know that they will receive any support and they have many opportunities for development. Majority in this department sees that people are privileged over other components of the business and feel at home and safe.

8. How is risk managed in Pipedrive?

Answer "D" received the highest percentage of 47.3%, which is 8.6% higher than the average percentage for this answer. The G&A department believes that sharing information and knowledge is the best way to manage risk, so training and support can help minimize risks and negative impacts.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 43.9%, which is 7.3% higher than the average percentage for this response. This demonstrates that in this department, people think that the rewards as well as the negative consequences should be shared among everyone, because everyone takes responsibility.

10. How performance evaluated in Pipedrive?

The answer "D" received the highest percentage of 39.5%, which is 5.9% higher than the average percentage for this response. People in this department believe that performance is measured by the community. And success is determined by shared values and shared responsibilities.

Appendix 10 – Analysis of Information Security Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 37.2%, which is 5.3% below the average percentage of 42.5% among all teams. This percentage indicates that a sense of community and shared security are valued within this team. The second highest percentage of 27%, which is 7% above the average for all teams, went to the answer "C". This response is related to the Culture of Autonomy, which means that flexibility and new approaches to solving issues are also highly valued in this team.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 39.6%, which is 5.7% below the average of 45.3% among all teams, which reveals that they see the benefits in teamwork and value cooperation, however, independent action is also welcome. This department sees that it is possible to succeed through human relations and support.

3. What does 'security' mean in Pipedrive?

The answer "B" received the highest percentage of 31%, which is 14.3% higher than the average 16.7% and the highest score 3.1 for this answer among all the departments. This is quite a big difference compared to other departments in how this department understands security in Pipedrive. Security means control, visibility and accountability especially for external entities. This shows that external requirements and rules must be met, as well as periodically undergo audits.

It is important to note that the "D" response received the lowest score of 2.4 among all departments, which reveals that security is not seen as a shared responsibility, at least not to a large extent.

4. How is information managed and controlled in Pipedrive?

The answer "A" received the highest percentage of 33%, which is % higher than the average percentage of 22.7% among all other departments, which means that information should be controlled and managed through policies and procedures, just like any other business assets. The lowest score for this question was 'D', which shows that this department believes that information should be restricted, protected, and not recklessly disclosed.

5. How are operations generally managed in Pipedrive?

The answer “B" and the answer “D” received equal 28.7%, which is higher by 8.3% for the answer “B” and lower by 3.7 for the answer “D” among the averages of all other departments. This shows that in Information Security department day-to-day operations need to be transparent, auditable and traceable to audits, while at the same time it is important that people can support each other in learning new skills and progressing in their careers.

6. How is technology managed in Pipedrive?

The answer "D" received the highest percentage of 29%, which is 2.5% below the average 31.5% among all the departments. Technology is perceived as an accessible tool for everyone and through technology education, people can maximize their productivity. In this department, technology is used to succeed and help achieve goals.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 44.4%, which means that teamwork is crucial in this department, where people receive special support and development opportunities, and are aware that everyone is contributing.

8. How is risk managed in Pipedrive?

The answer "C" received the highest percentage of 43%, which is by 22.3% above the average 20.7% for this response among all the departments. This is also the highest average score of 4.3 for this answer. This demonstrates that InfoSec department believes that risks are better managed by decentralized authority, and that risk-related decisions are better made by the people closest to the situation. It is important to note that the lowest percentage of 24% among all departments received a “D” response, which demonstrates that Infosec believes that sharing information, knowledge and responsibility with employees outside of security field is not the best way to manage risk and it has to be limited.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 32%, which shows that people in this department believes that accountability is shared among each other. Everyone makes decisions and does their job on the assumption that rewards and consequences are shared among the team.

10. How performance evaluated in Pipedrive?

Answer "C" received the highest percentage of 38.6%, which is 10.6% higher than the average of 28.3% for this answer. The people in InfoSec department see performance

evaluation as something about decisions and outcomes. Success in business is the main criterion.

Appendix 11 – Analysis of IT Ops Department

1. What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 35.2% for this question, however it is 7.3% below the average percentage of 42.5% among all teams. This percentage indicates that a sense of community is valued within this team, but shared security must be achieved through security awareness and informed decision making. The second-highest percentage of 29.6% was 7% above the average for all teams, and the highest among all departments went to an "A" response. This answer has to do with Process culture, meaning that transparency, stability, and reliability are also highly valued. IT Ops believes that knowing and following the rules is critical for everyone.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 40.4%, which is 4.9% below the average of 45.3% among all teams, which means that they see the benefits in teamwork and value cooperation, however, independent action is also welcome. Greater results can be achieved through human relations and support.

3. What does 'security' mean in Pipedrive?

The answer "D" received the highest percentage of 33.3%, which is 4.7% below the average 38% among all the departments. Security is perceived as security awareness, where everyone is more or less informed, active and, if necessary, ready to protect the company.

4. How is information managed and controlled in Pipedrive?

The answer "B" received the highest percentage of 32.5%, which is 2.5% higher than the average percentage of 30% among all other departments, which demonstrates that for IT Ops, information is a protected resource that must be verified, controlled and documented for any review or audit.

5. How are operations generally managed in Pipedrive?

The answer "B" received equal 31.6%, which is higher by 11.2% higher than the average 20.4% among the all other departments. It is also highest score 3.6 for this response among all the department. This indicates that it is important in IT Ops that day-to-day operations are transparent, verifiable, traceable and documented for review by any external entities.

6. How is technology managed in Pipedrive?

The answer "C" received the highest percentage of 30.1%, which is 5.8% above the average 24.3% among all the departments. Technology is managed locally and innovation is encouraged to achieve the best results. Technology is seen as a tool, not a limitation.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 30.8%, which is 15.6%, which is below the average of 46.4%. This shows that teamwork and support is valued in this department, but they also believe that success also depends on the fact that everyone must show that they are fulfilling their obligations.

8. How is risk managed in Pipedrive?

The answer "A" received the highest percentage of 27.8%, which is by 9.8% above the average 18% for this response among all the departments.This is also the highest average score of 3.5 for this answer. This means that IT Ops believes that risks are best managed by standardizing processes to be able to control and predict negative impacts.

9. How is accountability achieved in Pipedrive?

The answer "B" received the highest percentage of 22.4%, which is 4.5% higher than the average of 17.9% for this answer among all departments. This is also the highest average score of 3 for this answer. This department believes to some extent that accountability is achieved through reviews, and when everyone is held accountable for their actions.

10. How performance evaluated in Pipedrive?

Answer "A" received the highest percentage of 32%, which is 9% higher than the average of 23% for this answer. This is also the highest average score of 4 for this answer. This means that in order to measure success or failure, performance must be assessed in relation to the goals set and the strategies developed.

Appendix 12 – Analysis of Marketing Department

1. What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 41.3%, which is also close to the average percentage of 42.5% among all teams, which shows that people valued the most, they are part of the community and have joint responsibility in Pipedrive.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 38.5%, which means that they prefer teamwork and value cooperation. This department sees the benefits in human relationships, in supporting each other and sharing responsibility. It is interesting to note that the "B" response corresponding to the Compliance Culture received 16.3%, which is 4% higher than the average of 12.3% and reveals that external requirements and feedback are present in this department to a greater extent than in another department.

3. What does 'security' mean in Pipedrive?

The answer "D" received the highest percentage of 35.6%, which is 2.4% lower than the average percentage for this answer, which means that they perceive security as a shared responsibility to some extent. It is interesting to note that the answer "B" received 19%, which is 2.5% above average, and is also the highest among almost all departments, with the exception of security departments, this demonstrates that for this department, security also shows that everything should be transparent and documented, because they represent the company to the outside world and want to make sure that the proper evidence is collected.

4. How is information managed and controlled in Pipedrive?

The answer "B" received the highest percentage of 29.8%, which is close to the average of 30%, which indicates that the information is treated as a confidential and protected resource. In this department, people are constantly in contact with external parties, so they understand the importance of the integrity of information, because it is subject to verification and external audit.

5. How are operations generally managed in Pipedrive?

The answer "C" received the highest percentage of 32.7%, which is 4.9 higher than the average of 27.8% among all other departments. This reveals that it is preferable to have less bureaucracy and more freedom in day-to-day operations. Flexibility and innovation are highly prioritised in decision-making processes.

6. How is technology managed in Pipedrive?

The answer "D" received the highest percentage of 28.3%, which means that the technology is perceived as an accessible tool for everyone. In this department, technology is used to improve the success of internal stakeholders and maximize productivity.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 39.8%, which is 6.6 below the average of 46.4% among all departments. All other answers received approximately 20% each and are almost equal. This shows that teamwork and support for each other is important, but other aspects of people management must also be present, such as people following the rules, showing that they are doing the right thing and that they can make decisions quickly.

8. How is risk managed in Pipedrive?

The answer "D" received the highest percentage of 33%, which is 5.7% lower than the average of 38.7% among all other departments. The answer "B" also received a high percentage of 28.3%. This reveals that people in this department feel that risk is best managed by not only sharing knowledge and information, but also by gathering proper documentation, having frameworks and constant evaluations.

10. How performance evaluated in Pipedrive?

The answer "D" received the highest percentage of 32.4%, indicating that the performance is evaluated by the Pipedrive's community and in terms of successful decisions and excellent results that lead to business growth.

Appendix 13 – Analysis of Product Design Department

1. What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 50%, which is 7.5% higher than the overall average percentage of 42.5% among all departments. This demonstrates that a sense of family and shared community is very important to them. Human development and provided opportunities in the Pipedrive are also highly valued.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 51%, which is 5.7% higher than the average percentage for this answer. This reveals that people in the product design department view their work as a team effort, the value of which is that everyone benefits from such cooperation and constantly supports each other to achieve common goals. It is interesting to note that the answer "C" received 36.5%, which is the highest among all departments for this answer. Since this team is responsible for creativity, it is also important for them to have the freedom to make decisions and be able to act independently.

3. What does 'security' mean in Pipedrive?

The "D" answer received the highest percentage of 50.9%, which is 12.9% higher than the average percentage for this answer. This means that they see security as an awareness and shared responsibility where everyone has a role to play in protecting Pipedrive.

4. How is information managed and controlled in Pipedrive?

The "D" response associated with Trust Security Culture received the highest percentage of 32.8%, which is 4.6% higher than the average percentage among all other departments. This indicates that the Product Design department sees information as an important shared resource that helps improve productivity and plays an important role in empowering people, which leads to business success.

5. How are operations generally managed in Pipedrive?

The "D" answer received the highest percentage of 30.2%, which is 2.4% higher than the average percentage for this answer. This demonstrates that day-to-day operations in this department are flexible, with minimal restrictions and bureaucracy. Decisions are made based on the current situation and can be adapted to any environment.

6. How is technology managed in Pipedrive?

Answer "D" received the highest percentage of 32.1%, which is 0.6% higher than the average percentage for this answer. In this department, technological freedom is highly valued, where technology is available to everyone, and everyone should benefit from it in order to achieve maximum productivity.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 57.4%, which is 11% higher than the average percentage for this answer. This means that teamwork is highly valued and people know that they will receive any support and they have many opportunities for development.

8. How is risk managed in Pipedrive?

Answer "D" received the highest percentage of 50%, which is 11.3% higher than the average percentage for this answer. The Product Design department believes that sharing information and knowledge is the best way to manage risk, and proper training with support can help minimize risks and negative impacts.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 50.5%, which is 13.9% higher than the average percentage for this response. This reveals that people in this department believe that the rewards as well as the negative consequences should be shared among everyone because everyone takes responsibility. It is interesting to note that the answer "C" received 14.7, which is the lowest percentage among all faculties. This shows that results orientation is much less present than in other departments.

10. How performance evaluated in Pipedrive?

The "D" answer received the highest percentage of 46.3%, which is 12.7% higher than the average percentage for this answer. Performance is measured by the Pipedrive community, where success is determined by shared values and respect within the company.

Appendix 14 – Analysis of Product Org Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 36.2%, which is 6.3% below the average percentage of 42.5% among all departments, which means that people and the feeling of a family where everyone is in it together and support each other, are valued in this department. The other 3 responses received over 20% each, which demonstrates that these values also influence day-to-day decision making.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 37.4%, which shows that they prefer teamwork and value cooperation. This department sees the benefits in human relations, however, independent action is also welcomed, this can be seen as the answer "C" also received a rather high percentage of 29.9%.

3. What does 'security' mean in Pipedrive?

Answer "A" received the highest percentage of 35.7%, which is 7.9% higher than the average percentage for this answer. This indicates that security is perceived as rules, standards, policy enforcement, and where possible the use of automated infrastructure to protect information assets.

4. How is information managed and controlled in Pipedrive?

Answer "A" received the highest percentage of 29.1%, which is 6.4% higher than the average percentage of 22.7% among all other departments, which demonstrates that rules and policies play the most important role in information management. Information must be controlled and accounted for, it must be used as a valuable commodity.

5. How are operations generally managed in Pipedrive?

The answer "D" received the highest percentage of 30.4%, which reveals that the day-to-day activities in this department are conducive and supportive, allowing employees to learn new skills and responsibilities that can lead to career advancement at Pipedrive. It is interesting to note that the answer "A" received the highest percentage of 26.8% among all departments, which also means that daily activities must be predictable and follow the same rules and standards throughout Pipedrive.

6. How is technology managed in Pipedrive?

Answers "A" and "D" received the highest equal percentage of 26.1%, which shows that even though the technology is perceived as an accessible tool for everyone, it must be centrally managed and comply with standards and policies.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 35.5%, which is 10.9% below the average percentage of 46.4 among all departments. This indicates that teamwork with support and opportunities for growth are quite important in this department.

8. How is risk managed in Pipedrive?

The answer "D" received the highest percentage of 35.2%, which is 3.5% below the average percentage of 38.7% among all other departments. This demonstrates that this department believes that it is best to manage risk if everyone shares knowledge, experience and information. However, the other "A" and "B" responses also received high percentages compared to the averages of these responses, which means that standardization and regular assessments can also be very helpful in risk management.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 30.1%, which is 6.1% lower than the average of 36.6% among all other departments. This shows that everyone makes decisions and does their job on the basis that responsibility and therefore rewards and consequences are shared among the entire team.

10. How performance evaluated in Pipedrive?

The answer "C" received the highest percentage of 34.5%, which is 6.2% higher than the average of 28.3% among all other departments. This reveals that the measurement of performance is defined in terms of the decisions made and specific results that lead to the success or failure of some aspect of the business.

Appendix 15 – Analysis of Product Research Department

1. What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 45.5%, which is 3% higher than the average percentage of 42.5% among all teams, which means that people are most valued in Pipedrive. It's like a family, but in the workplace, where everyone helps each other and shares the responsibility.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 39.6%, which is 5.7 below the average percentage of 45.3% among all other departments. This indicates that they usually work as a team and cooperate well with each other. This department sees the benefits in human relationships, in supporting each other and sharing responsibility.

3. What does 'security' mean in Pipedrive?

Answer "A" received the highest percentage of 35.4%, which is 7.6% higher than the average percentage for this answer, which shows that they perceive security as a standard to the maximum automated process that should be set in accordance with policies and procedures.

4. How is information managed and controlled in Pipedrive?

The answer "D" received the highest percentage of 33.1%, which is 4.9% above the average of 28.2%, which reveals that information is seen as a shared resource and should be used to support people's productivity. Information must be available to everyone in Pipedrive to empower people to succeed.

5. How are operations generally managed in Pipedrive?

The answer "D" received the highest percentage of 35.1%, which is 2.7 higher than the average of 32.4% among all other departments. This demonstrates that the day-to-day activities in this department are conducive and supportive, allowing employees to learn new skills and responsibilities that can lead to career advancement at Pipedrive.

6. How is technology managed in Pipedrive?

The answer "A" and "D" received the highest equal percentage of 32.5%, which reveals that even though the technology is perceived as an accessible tool for everyone, it must be centrally managed and comply with standards and policies.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 49.6%, which is 3.2% higher than the average of 46.4% across all departments. This indicates that teamwork and support for each other is very important. Special attention is paid to the growth of people and continuous learning.

8. How is risk managed in Pipedrive?

The answer "D" received the highest percentage of 47.5%, which is 8.8% higher than the average of 38.7% among all other departments. The Product Research department believes that sharing information and knowledge is the best way to manage risk, so training and support can help minimize risks and negative impacts.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 44.1%, which is 7.5% higher than the average percentage of 36.6% among all other departments. This reveals that people in this department believes that accountability is shared among each other. Everyone makes decisions and does their job on the assumption that rewards and consequences are shared among the team.

10. How performance evaluated in Pipedrive?

The answer "C" received the highest percentage of 35.8%, indicating that the measurement of performance is defined in terms of successful decisions and excellent results that lead to business growth.

Appendix 16 – Analysis of Support Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 53.3%, which is 10.8% higher than the overall average percentage of 42.5% among all departments. This shows that a sense of family and shared community is very important to them. Human development and provided opportunities in the Pipedrive are also highly valued.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 59.3%, which is 14% higher than the average percentage for this answer. This indicates that people in the Support department view their work as a team effort, the value of which is that everyone benefits from such cooperation and constantly supports each other to achieve common goals.

3. What does 'security' mean in Pipedrive?

The "D" answer received the highest percentage of 44.9%, which is 6.9% higher than the average percentage for this answer. This means that they see security as an awareness and shared responsibility where everyone has a role to play in protecting Pipedrive.

4. How is information managed and controlled in Pipedrive?

The "B" response related to compliance culture received the highest percentage of 40.4%, which is 10.4% higher than the average percentage among all other departments. This demostrates that the support department treats the information as a confidential and protected resource that is entrusted by others to Pipedrive and is therefore subject to external auditing and verification.

5. How are operations generally managed in Pipedrive?

The "D" answer received the highest percentage of 41.6%, which is 9.2% higher than the average percentage for this answer. This validates that day-to-day operations in this department are flexible, with minimal restrictions and bureaucracy. Decisions are made based on the current situation and can be adapted to any environment.

6. How is technology managed in Pipedrive?

Answer "D" received the highest percentage of 39.8%, which is 8.3% higher than the average percentage for this answer. In this department, technological freedom is highly valued, where technology is available to everyone, and everyone should benefit from it in order to achieve maximum productivity.

7. How are people managed in Pipedrive?

The "D" answer received the highest percentage of 52.3%, which is 5.9% higher than the average percentage for this answer. This means that teamwork is highly valued and people know that they will receive any support and they have many opportunities for development. It is interesting to note that the answer "C" received the lowest percentage among all departments related to the Autonomy Culture. This demonstrates that people prefer team decisions over individual decisions and the associated risks.

8. How is risk managed in Pipedrive?

Answer "D" received the highest percentage of 44.6%, which is 5.9% higher than the average percentage for this answer. The Support department believes that sharing information and knowledge is the best way to manage risk, and proper training with support can help minimize risks and negative impacts.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 30%, which is 6.6% lower than the average percentage for this response. This reveals that people in this department believe that the rewards as well as the negative consequences should be shared among everyone because everyone takes responsibility.

10. How performance evaluated in Pipedrive?

The answer "D" received the highest percentage of 45%, which is 11.4% higher than the average percentage for this answer, and it is also the highest percentage among all other departments. Performance is measured by the Pipedrive community, where success is measured by shared values and mutual respect.

Appendix 17 – Analysis of Engineering Department

1.What's valued the most in Pipedrive?

The answer "D" received the highest percentage of 41.5%, which is 1% below the average percentage of 42.5% among all teams. This percentage indicates that sense of family at workplace and shared responsibilities are highly valued.

2. How does Pipedrive generally work?

The answer "D" received the highest percentage of 42.5%, which is 2.8% below the average of 45.3% among all teams, which means that they see the benefits in teamwork and value cooperation. This department sees that it is possible to succeed through human relations and support.

3. What does 'security' mean in Pipedrive?

The answer "D" received the highest percentage of 36.4%, which is 1.6% below than the average 38% among all the departments. This shows that people in Engineering department see security as an awareness and shared responsibility where everyone has a role to play in protecting Pipedrive.

4. How is information managed and controlled in Pipedrive?

The answer "B" received the highest percentage of 30.6%, which is 0.6% higher than the average percentage of 30% among all other departments, which reveals that information is perceived as a confidential resource entrusted to Pipedrive by external parties and, therefore, information and use of information should be well protected, documented and verified.

5. How are operations generally managed in Pipedrive?

The answer "C" received the highest percentage of 30.5, up 2.7% above the average percentage of 27.8% among all other departments. This demonstrates that in the engineering department, day-to-day activities should be with a minimum of bureaucracy, where it is possible to quickly adapt and be flexible if necessary.

6. How is technology managed in Pipedrive?

The answer "D" received the highest percentage of 29%, which is 2.5% below the average of 31.5% among all departments. Technology is perceived as an accessible tool for everyone and through technology education, people can maximize their productivity. In this department, technology is used as an aid to achieving goals and success.

7. How are people managed in Pipedrive?

The answer "D" received the highest percentage of 44.3%, which is 2.1% below the average among all other departments. This means that teamwork is quite important in this department, where people receive exceptional support and growth opportunities, and are mindful that everyone is contributing.

8. How is risk managed in Pipedrive?

The "D" response received the highest percentage of 35.3%, which is 3.4% below the average of 38.7% for this response among all departments. This indicates that this department believes that it is best to manage risk if everyone shares knowledge, experience and information. It also gives a sense of shared responsibility, which in some cases can lead to minimal individual accountability.

9. How is accountability achieved in Pipedrive?

The answer "D" received the highest percentage of 36%, which shows that people in this department believes that accountability is shared among each other. Everyone makes decisions and does their job on the assumption that rewards and consequences are shared among the team.

10. How performance evaluated in Pipedrive?

Answer "D" received the highest percentage of 32.4%, which is 1.2% lower than the average of 33.6% for this answer. This reveals that performance is evaluated by the Pipedrive community and shared commitment to a cause determines success.

Appendix 18 – Summary of the Analysis for each Department

Business Intelligence

There are 29 people in the whole department, of which 6 responded to the questionnaire, which is 21% of the acceptable response rate. Detailed analysis in Appendix.

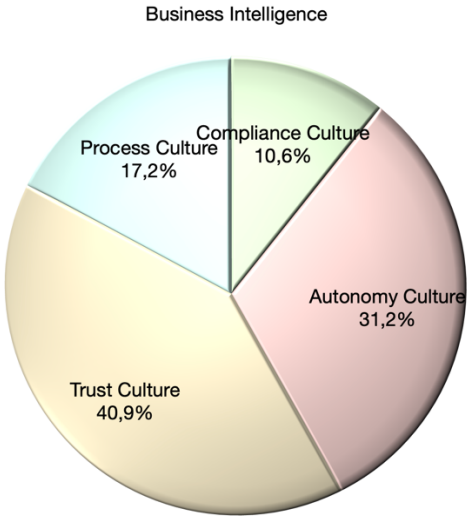

Figure 20. Business Intelligence Department

The dominant security culture present in this department is a Trust Security Culture with 40.9% , which is above the average percentage for this culture by 3.6%. This indicates that there is very strong focus on understanding people, trusting them and providing them support in whatever they might need. This culture supports ownership and shared responsibility while promoting growth and collaboration. People have a lot of faith in the Trust Culture because they believe everyone makes well-informed decisions.

The second largest culture that is present is Autonomy Security Culture 31,2% with the score 3.2, which is above the average percentage for this culture by 8.2%. This is very high discrepancy from the average percentage for Autonomy Culture, which shows the less desire for centralised control, therefore flexibility and adaptation to ever changing environment is valued the most. Promoting agility and supporting innovation are the core traits for the business success and development in Autonomy Security Culture.

The next culture represented in the Business Intelligence department is the Process Security Culture with a score of 1.8, representing 17.2% of all cultures present. This

percentage is less than the average percentage for this culture by 3.6%, which can be quite obvious because there is a high culture of autonomy in the department, and these cultures have conflicting values. In a Process Culture, security operations are managed under centralized control, maintaining existing structures over time and avoiding uncertainty and risk by enforcing policies is essential. On the other hand, the Autonomy Culture values and encourages more flexibility and innovation, and favors as little bureaucracy as possible. This reveals that for some processes central visibility and common practices are preferred, while for other processes new approaches and flexibility are welcome.

The lowest scores were received by responses related to Compliance Security Culture, 1.1 points, which is 10.6% of all cultures present. It is also the lowest percentage among all the departments for this culture. This demonstrates that the Business Intelligence department has very limited demand for requirements set by others outside of their organization, such as customers, business. Also, it shows that documenting and tracking evidence of operational processes and replicating processes on demand for external audit purposes is not very practical in this department.

Customer Success

In total, there are 27 people in the department, however 29 people answered the questionnaire, which is 107% of the acceptable percentage of responses for analysis. It is possible that some employees from other departments mistakenly noted that they belong to this department, but still the author will analyze the results, because the number of answers is more than sufficient. Detailed analysis in Appendix.

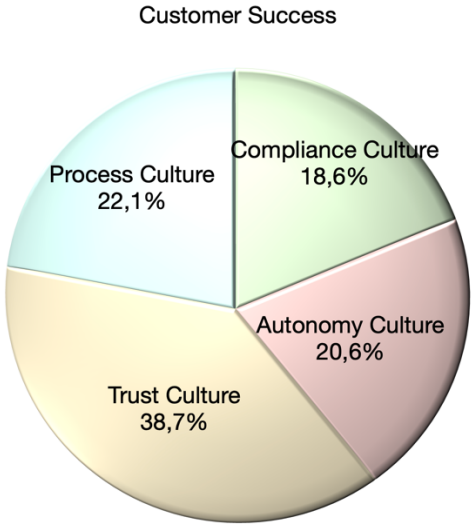

Figure 21. Customer Success Department

The dominant security culture present in this department is the Trust Security Culture, accounting for 38.7% of all other existing cultures. This is slightly higher than the overall average percentage for this culture, which is 37.3%, and indicates a greater value in empowering people by supporting them, encouraging them to take responsibility, and giving people everything they need to be security team allies. It is important to build a good internal security community in order to maintain a Trust Culture in the Customer Successs department as they interact a lot with outside parties and act as the first line of defense against external threats.

The second dominant culture present is the Process Culture with 22.1%, this is slightly above the overall average of 1.3%, which is 20.8%. This percentage reveals that this department values stability and visibility in security operations and sees security as a corporate function that should be coordinated in the same way everywhere.

The next culture represented is Autonomy Security Culture with 20.6%, which is 2.4% less than the average of 23% among other departments. This reinforces what was said above regarding the Process Security Culture that people in this department view security operations as a more centralized function and prefer to standardize security processes.

The culture with the lowest percentage of 18.6% is the Compliance Security Culture, slightly below the average overall percentage by 0.3%. This demonstrates that compliance requirements from outside Pipedrive do not exist or are limited and not as valued as the internal security environment, and the commitment to a Trust Culture is far above any external requirements placed on them.

Finance

In total, there are 15 people in the department, and 8 people answered the questionnaire, which is 53% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

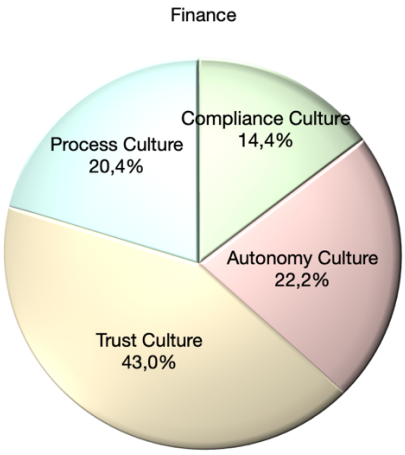

Figure 22. Finance department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 43% of all other existing cultures. This is 5.7% above the overall average percentage for this culture, which is 37.3%. This shows that people in the Finance department consider their environment as family and invest most of themselves in teamwork and in Pipedrive. Human relations and collaborative processes play a central role in the Trust Security culture. People are seen as security advocates, not threats. People in the Finance department understand the importance of security, and by empowering them with the finest training and tools, they will be able to make better security decisions.

The second dominant culture present is the Autonomy Security Culture with 22.2%, which is 0.7% below the overall average of 23%. This culture indicates that people prefer less centralized control and see the value in individual autonomy, where people can decide security issues themselves. Autonomy Security Culture is often present to some extent in tech startups where you have a limited number of people but they have enough experience to make security decisions. Since the percentage of this culture is below the overall average, this indicates that while members of the Finance department value less centralized control, they understand the risks associated with an Autonomy Security Culture.

The next culture represented is Process Security Culture with 20.4%, down by 0.4% from the average of 20.8% among other departments. This culture is close in percentage to the culture of autonomy, which reveals a kind of interchange between cultures, where stability is also valued as flexibility, but agility is slightly preferred over standardization.

The culture with the lowest percentage of 14.4% is a Compliance Security Culture, which is 4.4% below the overall average of 18.9%. This demonstrates that compliance requirements from outside of Pipedrive in Finance Department do not exist or are limited and that security issues related to concerns from other stakeholders, whether customers or regulators, may not be fully defined.

G & A

In total, there are 15 people in the department, however 18 people answered the questionnaire, which is 120% . It is possible that some employees from other departments mistakenly noted that they belong to this department, but still the author will analyze the results, because the number of responses is more than sufficient. Detailed analysis in Appendix.

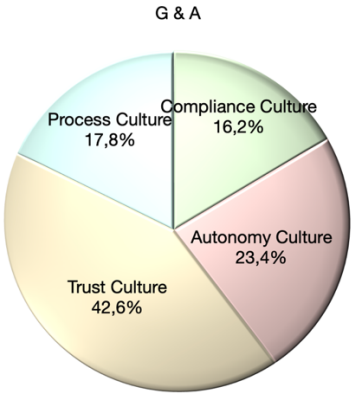

Figure 23. G & A department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 42.6% of all other existing cultures. This is 5.3% above the overall average percentage for this culture, which is 37.3%. It is interesting to note that for all 10 questions, the highest scores were obtained for answers related to the Trust Culture. This indicates that people in the G&A department put a lot of themselves into teamwork. Human relations, collaborative processes and shared security play a central role in the G & A. People are seen as security advocates, not threats.

The second dominant culture present is the Autonomy Security Culture with 23.4%, which is 0.4% above the overall average of 23%. This culture shows that people prefer less centralized control and see the value in individual autonomy, where people can make

decisions on security issues themselves. Autonomy Security Culture is often present to some extent in tech startups where you have a limited number of people but they have enough experience to make security decisions. Because Pipedrive is a tech unicorn that has grown rapidly over the past few years from a couple of hundred people to 900+, the Autonomy Security Culture is still very pervasive.

The next culture represented is Process Security Culture with 17.8%, which is 3% below the average of 20.8% among other departments. This precentages reveals that centralised management, policies and procedures are not the priority values for G & A. This department believes that communication, participation, flexibility and innovation are more helpful in achieving success and growth than standardization.

The culture with the lowest percentage of 16.2% is a Compliance Security Culture, which is 2.7% below the overall average of 18.9%. This exposes that compliance requirements from outside parties in G & A department do not exist or are limited and that security issues related to concerns from other stakeholders, whether customers or regulators, may not be relevant to them.

Information Security

In total, there are 20 people in the department, and 7 people answered the questionnaire, which is 35% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

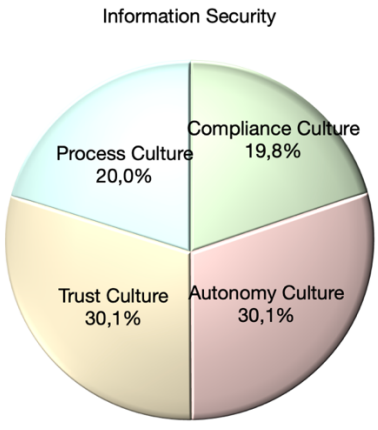

Figure 24. Information Security department security culture overview

There are two dominant security cultures present in this department, one is Trust Security Culture 30.1% and the second one is Autonomy Security Culture 30.1%. The Trust Culture is lower by 7.2% than the average percentage for this culture, which is quite significant difference. This reveals that the information security department does not have much trust in people who do not deal with security issues, preferring to control people's behavior, rather than letting them take responsibility for security issues. This is an important difference in how information security personnel see information security and the rest of the organization. Where security professionals see information security as locking things down, but others see it as a shared resource and see great value in a trusting community. The information security team may see more risks in sharing knowledge and information than benefits.

The Autonomy Security Culture is 7.1 percent greater than the average, indicating a significant divergence between the InfoSec and other departments. This does not necessarily show that the information security department is completely against bureaucracy and standards, but that they believe that there are different ways to manage security processes. Local and individual security management by a designated IT professional can be more successful in mitigating security risks. It is also possible that some freedom, such as using your own device and connecting to a corporate network, may not be considered a high security risk.

The third culture present is the Process Security Culture with 20%, which is 0.8% below the overall average of 20.8%. Such a percentage demonstartes the limited value of centralization and complete control over everyone and everything. However, it is important for InfoSec team that security operations be transparent and coordinated in order to minimize security risks. Also, it reveals that the department has processes and procedures in place, but not for everything.

The culture with the lowest percentage of 19.8% is a Compliance Security Culture, which is 1% above the overall average of 18.9%. Compliance Culture is present almost to the same extent as Process culture, only 0.2% less. This shows that there are compliance requirements from external entities such as regulatory bodies and ISOs, for the InfoSec department. Documenting and maintaining evidence of processes for external Pipedrive stakeholders should be done, but to a limited extent.

IT Ops

In total, there are 14 people in the department, and 5 people answered the questionnaire, which is 36% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

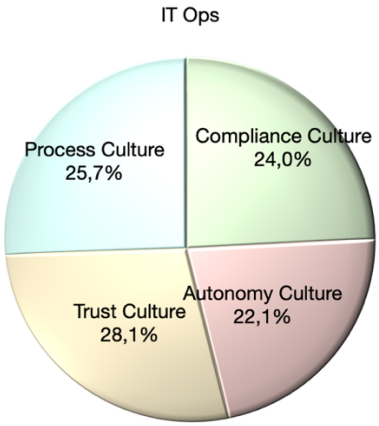

Figure 25. IT Ops department security culture overview

The dominant security culture present in this department, is the Trust Security Culture 28.1%. The Trust Culture is lower by 9.2% than the average percentage for this culture, which is quite significant difference. Although the Trust Culture is not as high as in other departments, human relations and empowerment of people are highly valued, but also centralized processes, procedures and control play an important role for IT Ops.

The second dominant culture is a Process Culture with 25.7%, which is higher by 4.9% than the average percentage for this culture and also the highest among all other departments. This department responsible for managing and coordinating information technology operations of a business to ensure optimal performance. Therefore, the stability and transparency of processes to maintain existing functions, predict results, and ensure standardization of rules are highly valued in IT Ops department.

The third culture represented is Compliance Security Culture with 24%, which is 5.1% higher than the overall average of 18.9% and the highest among all other departments. This percentage demonstrates that this department maintains frequent relationships with external organizations in terms of addressing the issues of external stakeholders such as

regulators or customers whose data is managed by Pipedrive. IT Ops ensure that there is proper documentation and predictable results that meet the expectations and requirements of external stakeholders.

The culture with the lowest percentage of 22.1% is an Autonomy Security Culture, which is 0.9% below the overall average of 23%. An Autonomy Culture means less centralized control, however, judging by the below average percentage for this department, standard security processes and other centralized control methods are more favorable than leaving security decisions to the discretion of the individual.

Marketing

In total, there are 61 people in the department, received 31 responses, which is 61% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

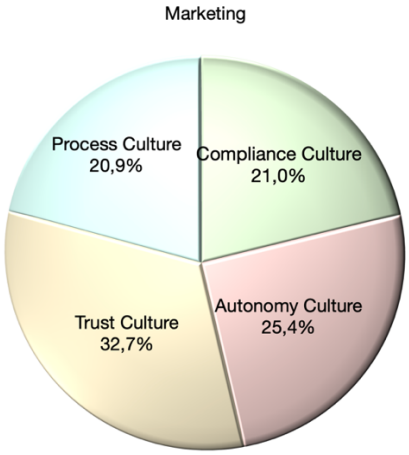

Figure 26. Marketing department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 32,7% of all other existing cultures. This is 4.6% below the overall average percentage for this culture, which is 37.3%. This indicates that people in the Marketing department see their environment as their own and invest most of themselves in teamwork and for the benefit of Pipedrive. Human relations and collaborative processes play a central role in the Trust Security culture. In Marketing department, people understand why security is important, and by providing them with the best training and the tools they need, it will help them make better security decisions.

The second dominant culture present is the Autonomy Security Culture with 25.4%, which is 2.4% above the overall average of 23%. This culture shows that people prefer

less centralized control and see the value in individual autonomy, where people can decide security issues themselves. Since the percentage of this culture is above the general average, this means that marketing staff value less centralized control and prefer to rely on individual security solutions.

The next culture represented is Compliance Security Culture with 21%, which is 2.1% above the average of 18.9% among other departments. This reveals that there are few compliance requirements and security issues related to external stakeholder concerns, whether customers or regulators in the Marketing Department.

The next culture is Process Culture which is very close in percentage to Compliance Culture, at 20.9%, which is 0.1% above the overall average. This demonstrates that centralized management, policies and procedures are of sufficient value and are present in the Marketing department to the same extent as the average throughout Pipadrive.

Product Design

In total, there are 53 people in the department, 12 people answered the questionnaire, which is 23% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

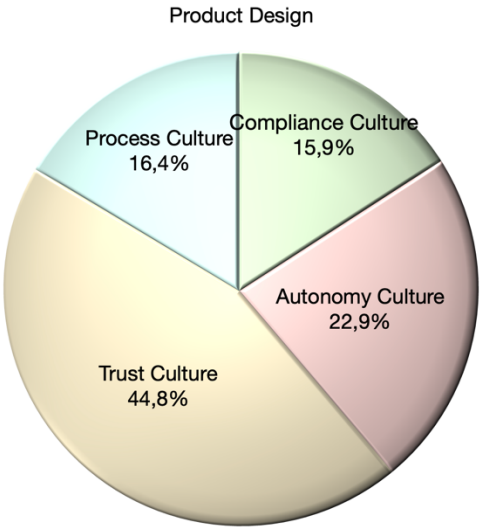

Figure 27. Product Design department security culture overview

The dominant security culture present in this department is a Trust Security Culture with 44.8% , which is above the average percentage for this culture by 7.5%. This culture

emphasizes human development and collaboration, and encourages ownership and shared responsibility. This points to the importance in this department of empowering people and supporting them with the skills and knowledge they need.

The second largest culture that is present is Autonomy Security Culture 22.9%, which is 0.1% below the average percentage for this culture. Mostly creative people work in this department, who, perhaps, have less craving for centralized control and standardization, they much prefer flexibility and innovation. Promoting agility and supporting innovation are the core traits for the business success and development in Autonomy Security Culture.

The next culture represented in the Product Design department is the Process Security Culture with a score of 1.8, representing 16.4% of all other cultures. This percentage is less than the average percentage for this culture by 4.4%, which can be quite obvious because there is a high culture of autonomy in the department, and these cultures have conflicting values. In a Process Culture, security operations are managed under centralized control, maintaining existing structures over time and avoiding uncertainty and risk by enforcing policies is essential. On the other hand, the Autonomy Culture values and encourages more flexibility and innovation, and favors as little bureaucracy as possible. This indicates that for some processes central visibility and common practices are preferred, while for most processes novel approaches and flexibility are welcome.

Almost equal percentage related to Compliance Security Culture, at 15.9%, which is 3% below of all other cultures. This means that the Product Design department has very limited demand for requirements set by others outside of Pipedrive. It also shows that documenting and tracking evidence of operational processes and replicating processes on demand for external audit purposes is not very practical in this department.

Product Org

In total, there are 55 people in the department, 22 people answered the questionnaire, which is 40% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

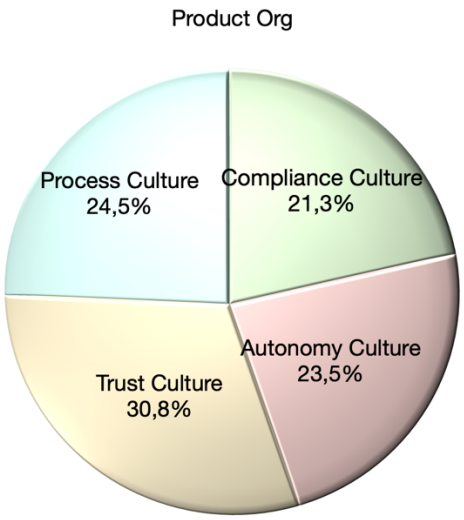

Figure 28. Product Org department security culture overview

The dominant security culture present in this department, is the Trust Security Culture 30.8%. The Trust Culture is lower by 6.5% than the average percentage for this culture, which is quite significant difference. Although the Trust Culture is not as high as in other departments, human relations and empowerment of people are highly valued, but also centralized processes, procedures and control play an important role.

The second dominant culture is a Process Culture with 24.5%, which is higher by 3.7% than the average percentage for this culture. This department responsible for managing and developing services and products to deliver maximum value to customers and ensure optimal success. Therefore, the stability and transparency of processes to maintain existing functions, predict results, and ensure standardization of rules are highly valued in Product Org department.

The third culture present is Autonomy Security Culture, which is 0.5% above the overall average of 23%. In this department, accountability and performance are assessed based on specific decisions and results of business success. However, judging by the answer to the security question, standard security processes and other methods of centralized control are preferable to leaving security decisions to individuals.

The culture with the lowest percentage of 19.8% is the Compliance Culture, which is 4.8% higher than the average percentage for this culture. This reveals that this department maintains frequent relationships with external organizations in terms of addressing the issues of external stakeholders such as regulators or also customers whose data is managed by Pipedrive.

Product Research

In total, there are 10 people in the department, received 7 responses, which is 70% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

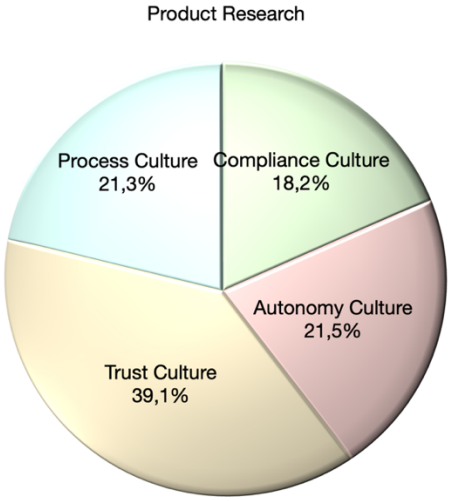

Figure 29. Product Research department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 39.1% of all other existing cultures. This is 1.8% above the overall average percentage for this culture, which is 37.3%. This demonstrates that people in the Product Research department put a lot of themselves into teamwork. Human relations, collaborative processes, as well as shared responsibilities play an important role in this department.

The second dominant culture is the Autonomy Security Culture with 21.5%, which is 2.5% below the overall average of 23%. Judging by the responses, the highest behavior of the Autonomy Culture is manifested in the evaluation of effectiveness, where it is based on actual decisions and successful outcomes.

The next culture represented is Process Security Culture with 21.3%, which is 0.5% above the average of 20.8% among other departments. The Process Culture is highly evident in the implementation of security and shows that people in this department highly value standard procedures, policies, and centralized control in all aspects of security management.

The culture with the lowest percentage of 18.2% is a Compliance Security Culture, which is 0.7% below the overall average of 18.9%. This reveals that compliance requirements

from external parties in Product Research department are limited and that security issues related to concerns from other stakeholders, whether customers or regulators, may not be directly related to or unknown to them.

Support

In total, there are 53 people in the department, 12 people answered the questionnaire, which is 23% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

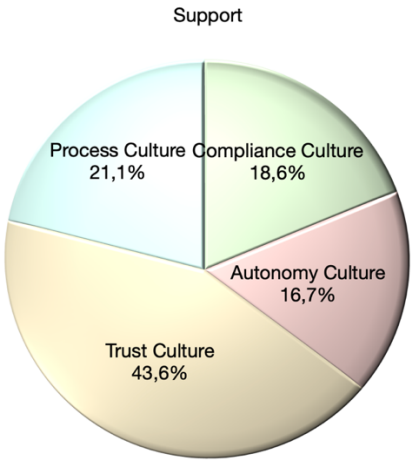

Figure 30. Support department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 43.6% of all other existing cultures. This is 6.3% above the overall average percentage for this culture, which is 37.3%. It is interesting to note that for 9 questions, the highest scores were obtained for responses related to a Trust Culture, and only for one question on information management, the highest score was received for a response related to a Compliance Culture, where employees of this department view information as a confidential resource, which has been entrusted to Pipedrive by external parties and must therefore be properly documented and verified. In addition, in the Support Department, human relations, collaborative processes, shared responsibility, where

everyone is also a stakeholder in ensuring security, play a central role. People are seen as security advocates, not threat actors.
The second dominant culture present is the Process Security Culture with 21.1%, which is 0.3% above the overall average of 20.8%. This culture indicates that people prefer centralized control and see value in standardization where people can follow existing security policies. However, it is interesting to note that this department also defines security as awareness and shared responsibility, which shows that they see the benefits of everyone's active participation in the defense of Pipedrive, although there may be some lack of knowledge about security risks.

The next culture present is Compliance Security Culture with 18.6%, which is 0.3% below the average of 18.9% among other departments. This demonstrates that regular external reviews in the Support department of some processes are limited, however, information management is subject to constant external reviews and audits and should be properly documented and verified.
The culture with the lowest percentage of 16.7% is an Autonomy Security Culture, which is 6.3% below the overall average of 23% and this is the lowest percentage among all other departments. Such a low percentage in the Support Department is explained by the customer support workflow, in which flexibility and innovation can lead to unjustified risks, respectively, well-structured procedures and transparency of operations are very important.

Engineering

In total, there are 374 people in the department, and 115 people answered the questionnaire, which is 31% and it is acceptable percentage of responses for analysis. Detailed analysis in Appendix.

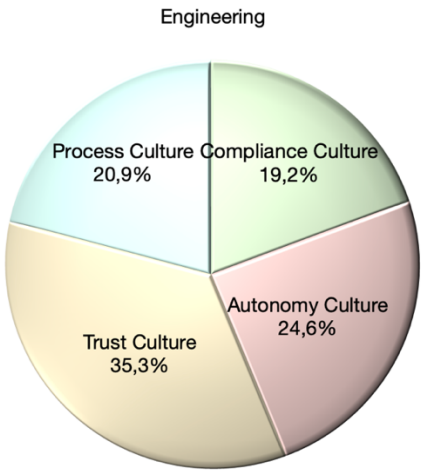

Figure 31. Engineering department security culture overview

The dominant security culture present in this department is the Trust Security Culture, accounting for 35.3% of all other existing cultures. This is 2% below the overall average percentage for this culture, which is 37.3%. This indicates that people in the Engineering department see their environment as their own and invest most of themselves in teamwork and for the benefit of Pipedrive. In the engineering department, people define security as a shared responsibility in which all members participate and collaborate as a team to ensure the success of the organization. However, for the successful implementation of the Trust Security Culture, everyone must have the necessary skills, knowledge and personal commitment to make the best security decisions.

The second dominant culture present is the Autonomy Security Culture with 24.6%, which is 1.6% above the overall average of 23%. This percentage demonstrates that people favor less central authority and value individual autonomy, where people, regardless of position, may choose for themselves what needs to be safeguarded and how.

The next culture is the Process Culture with 20.9%, which is 0.1% above the overall average. This shows that centralized management, policies and procedures are of sufficient value and they are present in the Engineering department to the same extent as the average throughout Pipadrive.

The culture with the lowest percentage of 19.2% is a Compliance Security Culture, which is 0.3% above the average of 18.9% among other departments. This means that the Engineering Department has limited compliance requirements associated with external stakeholders, whether those are customers or regulators.

Departments that did not receive a full analysis due to lack of sufficient responses or non-transparent results.

Biz Dev

This department has 2 active members, but 4 responses were received. This could be due to the fact that the questionnaire was completed twice by the same employees or employees from other departments mistakenly selected this department. Although it would be possible to analyze the responses by percentage, but in this team there is such a small number of participants and it is not clear who answered the survey, then an accurate picture of the existing security culture will not be visible.

For informational purposes only, and not for analysis, the author has included the following results. Based on the responses received, the distribution of security culture in this department is as follows: Compliance culture received the highest overall percentage of 28.8%, followed by Trust culture at 25.5%, followed by Autonomy Culture at 24.7%, and the lowest percentage was for Process Culture 21 .6%.

Channel and Partnerships

There are 9 people in this department, two of them answered the questionnaire. This is 22%, which is an acceptable response rate, however, the number of participants is not enough to conduct a meaningful analysis.

For informational purposes only, and not for analysis, the author has included the following results. Based on the responses received, the distribution of security culture in this department is as follows:

Trust Security Culture received the highest overall percentage 50% and it is highest amount all the departments. The second dominant culture is Autinomy Culture 33.5%, which is also the highest among all other departments. The Process Culture and Compliance Culture received the lowest percentages among other departments as well, 6% and 10.5% respectively.

Executive

There are 12 people in this department, two answered the questionnaire. This is less than 20%, which is below our acceptable level, and the number of responses is too low for a meaningful analysis.

For informational purposes only, and not for analysis, the author has included the following results. Based on the responses received, the distribution of security culture in this department is as follows: Trust Culture received the highest overall percentage of 29.5%, followed by Autonomy Culture 26.5%, followed by Process Culture 23.9% and the lowest percentage was for Compliance Culture.

People & Culture

Of the 48 employees of this department, six people answered the questionnaire. This is 13% of responses, which is below our acceptable level to draw conclusions based on the information collected.

For informational purposes only, and not for analysis, the author has included the following results. Based on the responses received, the distribution of security culture in this department is as follows: Trust Culture received the highest overall percentage of 42.8%, and an average score of 6, which is the highest score for the Trust Culture among all departments. Process Culture then scored 19.9%, followed by a nearly equal Autonomy Culture of 18.9% and Compliance Culture of 18.3%.

Revenue

There are 113 employees in this department, but only 5 responses were received. This is the lowest response rate of 4% in the entire organization. Therefore, a detailed analysis cannot be performed at such a low level of participation.

For informational purposes only, and not for analysis, the author has included the following results. Based on the responses received, the distribution of security culture in this department is as follows: Trust Culture scored the highest overall percentage of 41%, followed by Process Culture 22.3% and followed by Compliance Culture 21.1%. The answers for the Autonomy Culture received the lowest 15.6% and an average score of 1.6, which is the lowest score for the Autonomy Culture among all departments.

Appendix 19 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Nadezda Semjonova

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Guidelines for Developing Cyber Security Culture: the Case of Pipedrive OÜ”, supervised by Jesse Wojtkowiak and co-supervised by Kieren Nicolas Lovell.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

16.05.2022

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.