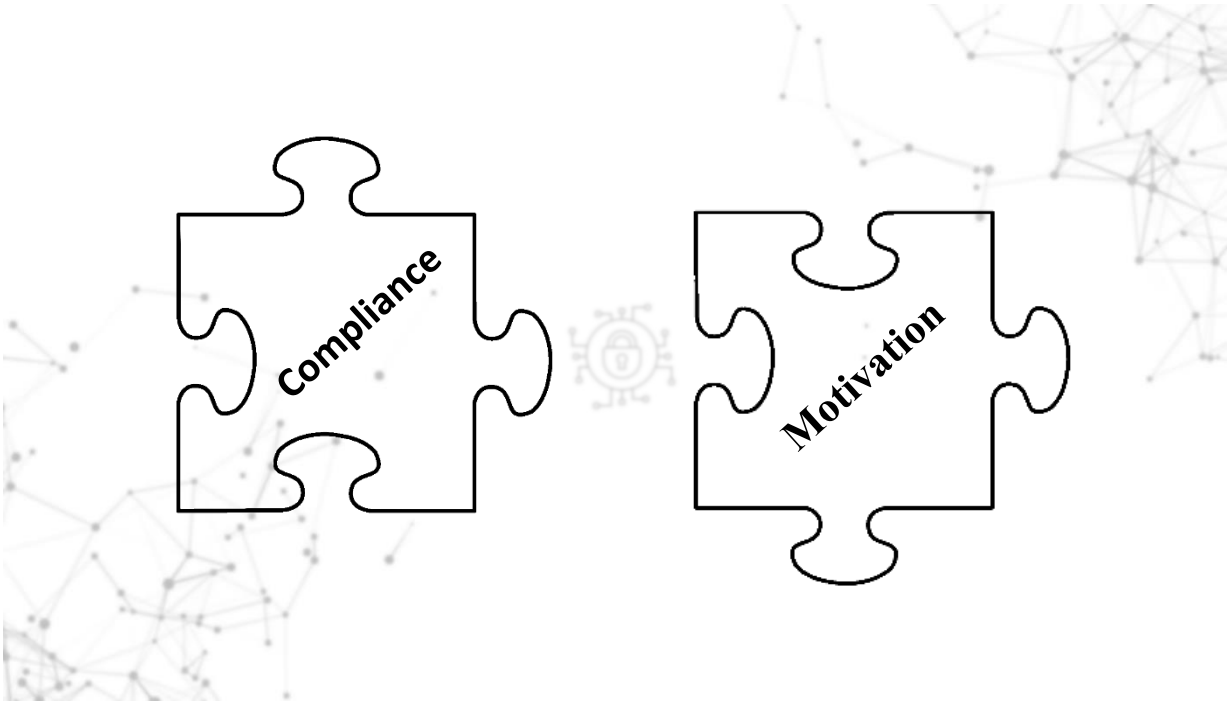
# Non-compliance with cybersecurity policies: Contributing factors of motivation (types)

Vollebregt, Arn

Name Arn Vollebregt
Date 17-08-2023
Version 1.0

# Non-compliance with cybersecurity policies

## Contributing factors of motivation (types)




https://www.pngitem.com/middle/TiRTxo_puzzle-piece-white-blank-white-puzzle-piece-transparent/
https://stock.adobe.com/nl/images/Cyber-security/179880629
https://wallpaperaccess.com/white-technology

**Keywords**: cybersecurity, compliance, motivation, extrinsic motivation, intrinsic motivation, General Deterrence Theory, Cognitive Evaluation Theory.

# Abstract

This study examines non-compliance with policy, or not following the rules, within the cybersecurity domain, which is commonly perceived as the cause of cybersecurity incidents. Specifically, it researches contributing factors of motivation. For this, literature from other domains is examined for approaches on using motivation to increase compliance, and whether these could be applied to cybersecurity. To this end the underlying theoretical frameworks of governance, policy, compliance, non-compliance, and motivation are first examined. The motivational approach to stimulate compliance with policy rules were identified as either extrinsic or intrinsic motivation. The former relies on incentives or deterrents, as stipulated by General Deterrence Theory (GDT), and is commonly employed in cybersecurity. The latter uses autonomy, competence, and relatedness from Cognitive Evaluation Theory (CET), which could be used as an alternative approach within cybersecurity. The different approaches from other domains which successfully increased compliance were examined and found to utilize alternative styles of governance, policy, communication, and education. These approaches could either directly or indirectly be related to CET, indicating viability for application in the cybersecurity domain. Based on this, alternative approaches for application to cybersecurity were hypothesized. Although further research for their application is required, the findings of this study provide a foundation for an alternative approach within cybersecurity which could improve compliance with cybersecurity policy.

# Table of Contents

# 1 Introduction

Cyberspace has proliferated throughout society over the last few decades, but not without its challenges. Cyber related technology and processes have become integral to everyday life privately, publicly, as well as commercially. It provides a gateway to friends and family, and all our electronic devices, but is also used for digital stalking. Governments use it to provide services to citizens and run elections, yet also to wage cyberwar on each other [1]. Businesses employ it to provide customers with entertainment, while datamining those same customers and expanding their global influence at the same time. This exposes us to risks as demonstrated by an abundance of cyber incidents. Personal devices are held captive virtually while their owners are extorted for ransom [2]. Critical infrastructure becomes unavailable either through collateral or intentional damage by cyberwar [3]. Supply chains are compromised and used either for hacking corporations or spying on rival nations [4]. These risks need to be managed, as cyberspace has become so intertwined with everyday life disconnecting is no longer an option.

Rules have been instituted by all parties in the cyberspace domain in order to minimize the risks associated with cyberspace. To be effective adherence to those rules is required, giving rise to the concept of compliance. These cybersecurity policies impose a wide variety of restrictions and tell people what to do and how to behave in certain situations. Online accounts should be protected by complex passwords of a certain length and complexity to avoid hackers guessing them. Citizens' Personal identifiable information (PII) is to be encrypted to prevent unauthorized access. Programming code contains intellectual property (IP) that must never be accessible directly via internet to maintain a competitive edge. However, people tend not to comply with these rules. Birthdays are easier to remember than complex passwords, but hackers can harvest this information from online social networks where people share this information [5]. Encryption of personal information is costly and complex, and 3rd parties may get hacked resulting in leakage of PII [6]. Product development during the COVID pandemic could only be performed by working from home due to lockdowns, which lead to exposure of IP [7]. Cybersecurity policies, backed by years of industry experience and practices, provides clear guidance on how to prevent such cyber incidents. So why do people sometimes not follow these rules, thus becoming non-compliant with cybersecurity policies?

The common perception is that users are the main culprit in cybersecurity incidents, which could have been prevented through policy adherence. They either have malicious intent, such as disgruntled employees, lack motivation, or do not possess the required knowledge. The accepted solution is security awareness training [8, p. 757]. This aims to underline the importance of cybersecurity, and thus adherence to cybersecurity policies, by providing education on the abundance of techniques used by hackers and teach users about cybersecurity measures that should be taken to prevent successful hacks. However, these widely applied trainings seem unable to stop the continued compromise of computers connected to cyberspace. Assuming these trainings are successful in imparting knowledge, the question regarding motivation remains. How are users stimulated for compliance? Are there perhaps alternative approaches to stimulate this, and could this lead to a different outcome? And most importantly: could this be applied to cybersecurity?

This study aims to research exactly that, by answering the following question: are other domains using motivation to increase compliance, what could be learned from their approach, could this be applied to cybersecurity, and if so: how?

## 1.1 Reading Guide

This introduction (chapter 1) provides a high-level overview of the problem of non-compliance in cyberspace and the research question of this thesis. Additionally, the research methodology (chapter 1.2) used in pursuit of an answer to this question is described.

The background (chapter 2) of the problem of non-compliance in cyberspace is decomposed into governance (chapter 2.1) from which stems policy (chapter 2.2) that requires compliance (chapter 2.3). Non-compliance (chapter 2.4) is then examined, along with the role motivation (chapter 2.5) plays in this.

Possible solutions (chapter 3) from other domains are examined and categorized into different solution directions. Governance (chapter 3.1) describes participation (chapter 3.1.1), self-regulation (chapter 3.1.2) and local rulemaking and monitoring (chapter 3.1.3). Policy (chapter 3.2) in turn details administrative burden (chapter 3.2.1) and gamification (chapter 3.2.2). Communication (chapter 3.3) covers framing (chapter 3.3.1), motivational interviewing (chapter 3.3.2), prosocial motivation (chapter 3.3.3) and autonomy-supportive behavior (chapter 3.3.4). Finally, education (chapter 3.4) outlines bias correction (chapter 3.4.1) and awareness training (chapter 3.4.2).

The discussion (chapter 4) then zooms out to place the possible solutions in the context of the background and hypothesizes on the feasibility of application within the cybersecurity domain. This is followed by the limitations (chapter 4.1) of this study and closed with a conclusion (chapter 4.3) containing answers to the research question.

Naturally, all sourced and referenced literature can be found in the bibliography (chapter 5).

## 1.2 Methodology

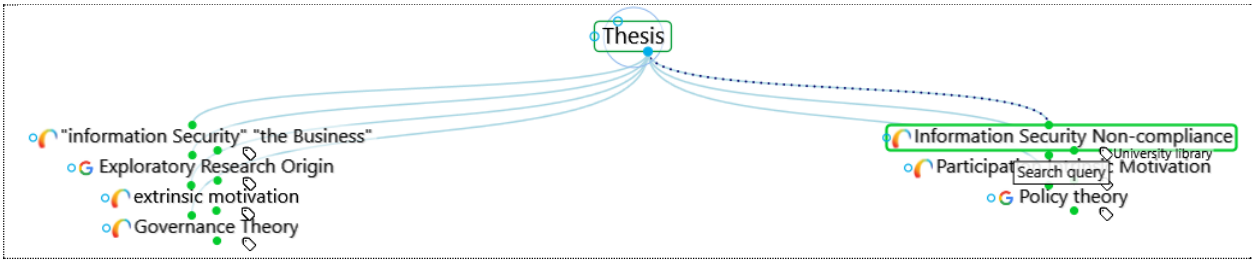
To research alternative solutions from other domains a literature study was performed. This allows for reuse of data, knowledge, and experience from previous studies and other domains to ascertain the feasibility of application in cybersecurity. This can then be researched further through future studies. The study was split into two stages. The first stage examined how motivational factors are related to (non-)compliance. For this, the construct of non-compliance was decomposed into its underlying theoretical frameworks by examining literature. The idea of compliance was disentangled from the concept of policy, or rule setting, upon which adherence depends. Policy was then detached from the concept of governance, from which these rules originate. These theories were then contrasted with the reality of non-compliance. Motivation was examined as a potential contributing factor, based on the common notion that “lack of motivation” contributes to non-compliance [9, p. 102]. This uncovered the differentiation between extrinsic motivation and intrinsic motivation, the latter of which is part of Cognitive Evaluation Theory (CET). The second stage of the study examined research from other domains that utilized alternative approaches for remediating non-compliance. These domains were selected based on a reasonable assumption of encountering the existence of compliance issues, such as in safety and healthcare. Alternative approaches were then studied for their underlying theoretical frameworks, how they increased compliance, and potential application to cybersecurity. The approach to this differed based on the type of research encountered. Successfully applied interventions from experiments were studied directly for applicability. For surveys and questionnaires, the contributing factors to success were studied for applicability, to be able to hypothesize tangible interventions based on their relative abstract content. Additionally, results from both were correlated

with observations and findings from the first stage, highlighting relations between their theoretical frameworks and any contributing factors to CET. The findings of this study can, in turn, provide a foundation for future scientific study as well as practical application.

The literature research was conducted online using the University Leiden Library Catalogue[1] and the Google search engine[2]. The following initial search terms were used, inspired by the research question:

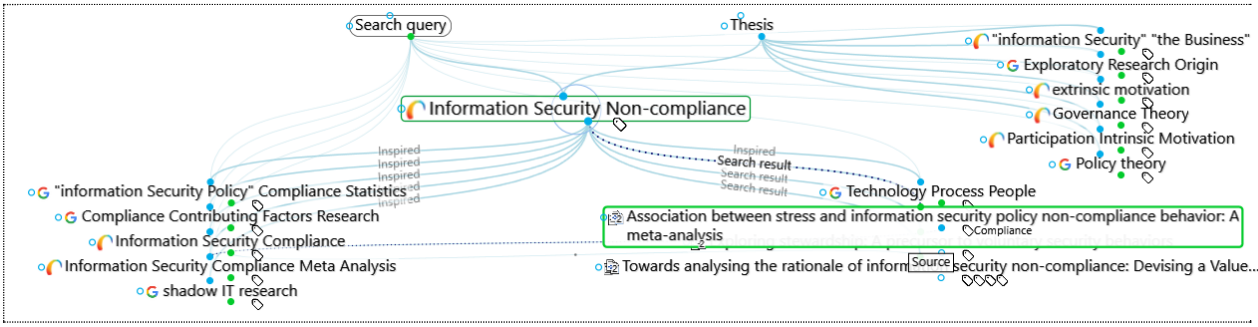
- Information Security Non-compliance
- Extrinsic motivation
- Participation Intrinsic Motivation
- Governance Theory
- Policy Theory

The abstracts of the top 50 search results were then manually reviewed for relevance to the research question. This was determined based on coverage of concepts such as (non-)compliance, motivation, and participation/collaboration as well as novelty in relation to cybersecurity approaches. Additionally, the scoping of these concepts was examined, which could be too narrow/specialized or too broad to be transferable to cybersecurity. Sources deemed relevant were used either as reference, provided their own references for additional research, or inspired subsequent search terms subjected to the same criteria. The following domains were sourced for studies and deemed a broad enough cross section for alternative approaches: universities, healthcare, safety, defense, law enforcement, technology, psychology, nature preservation, agriculture, retail, and the maritime industry. Finally, studies within the cybersecurity domain were treated with caution as this signaled existing application within this domain, thus providing less relevance for exploration of new approaches within this domain. The results of this process has been documented using TheBrain[3], a knowledge and relationship management tool with similarities to mind mapping. The following image displays the initial search terms (some of which were placed outside of scope during the evolution of this thesis):

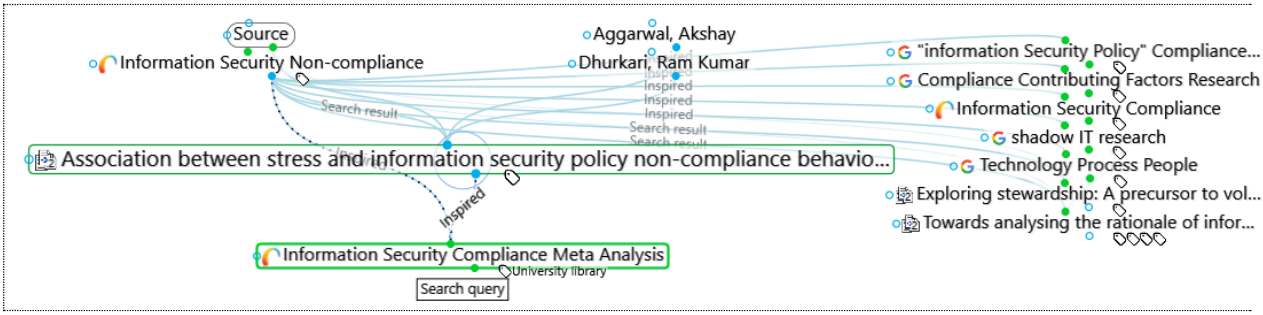



Zooming in on the search term ‘Information Security Non-compliance’ there were a number of relevant search results as well as follow-up search terms inspired by it:

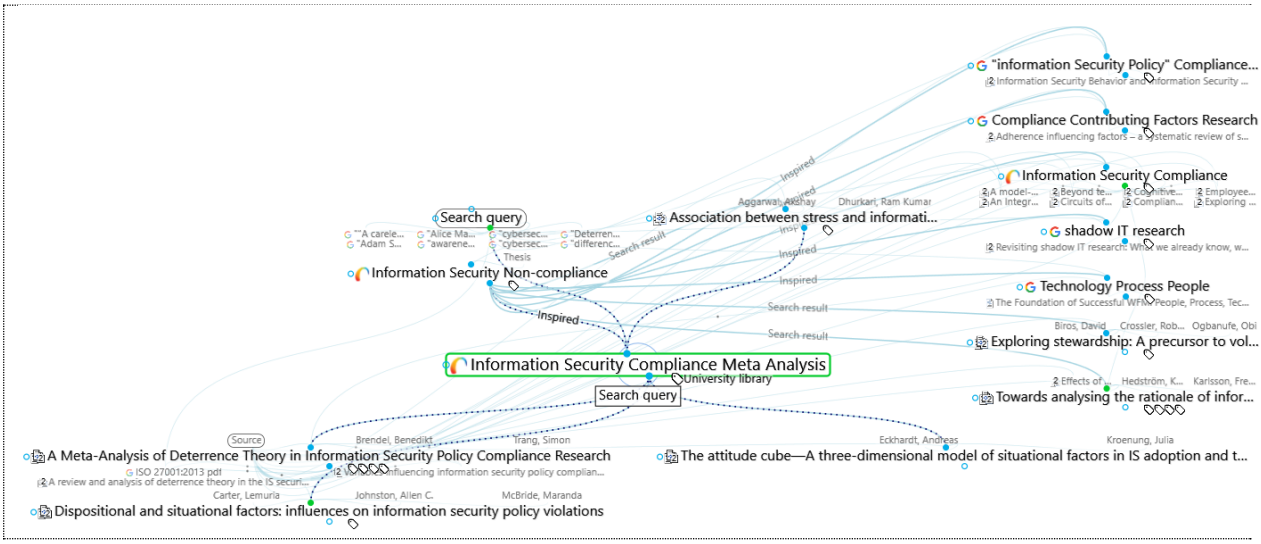
[1] https://catalogue.leidenuniv.nl/
[2] https://www.google.com/
[3] https://www.thebrain.com/, proprietary software requiring a license.




Examining one of the relevant sources ('Association between stress and information security policy non-compliance behavior: A meta-analysis'), a follow-up search term ('Information Security Compliance Meta Analysis') is displayed:

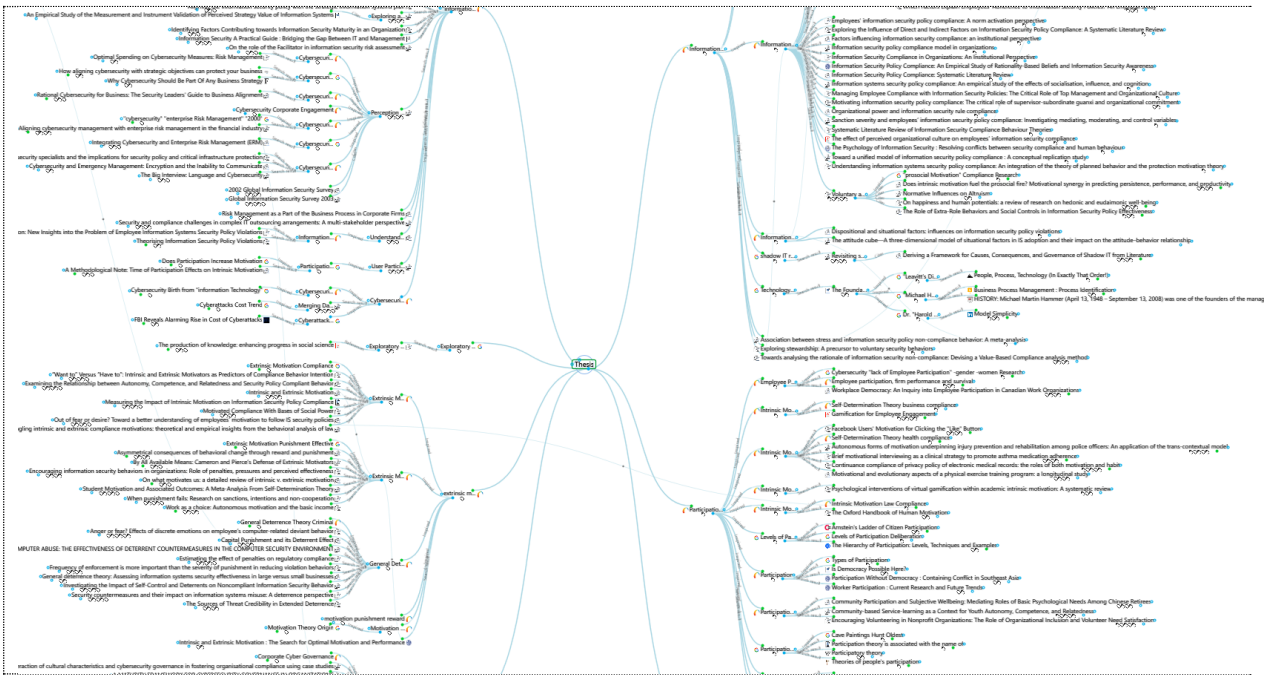



This in turn yields several relevant sources, displayed here with 2nd degree relationships to other sources and search terms:



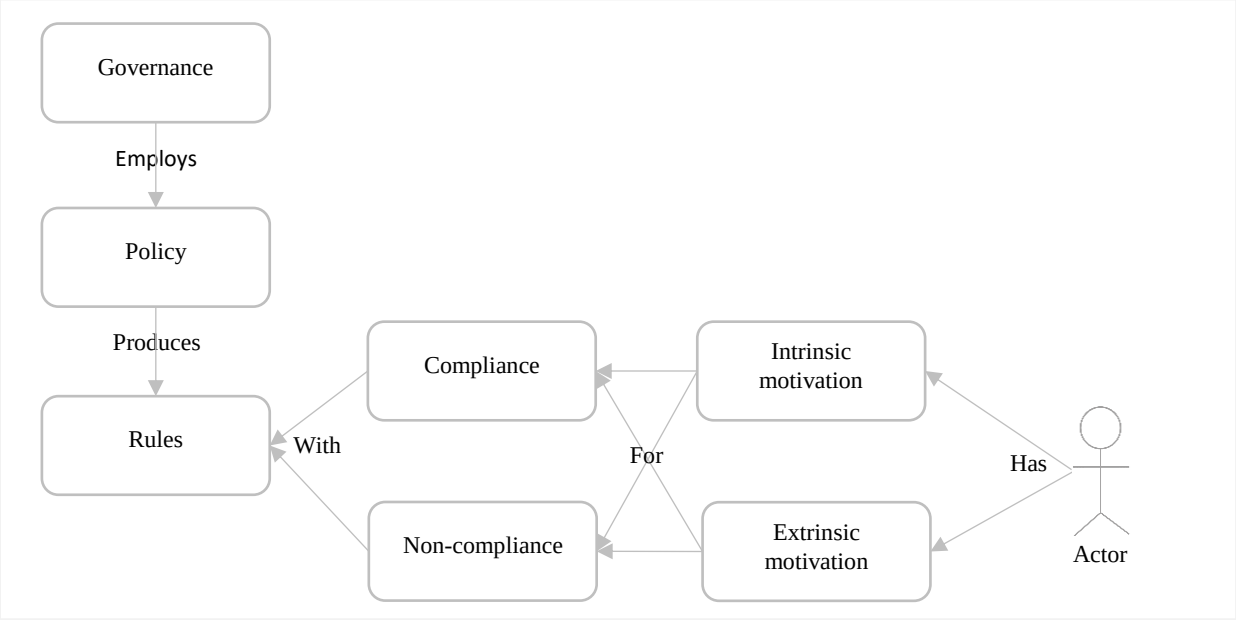

The resulting knowledge database is available on request in .brz format, a Brain archive. The screenshots provide a limiting overview of all results and omits some information as well as relationships beyond the nth degree, as can be seen in the overview below:

Name Arn Vollebregt
Date 17-08-2023
Version 1.0



# 2 Background

Before researching cybersecurity compliance its context must be touched upon. Whether (or not) to abide by a rule is not only driven by circumstances, but also by the motivation to do so. This (non-)compliance (chapter 2.3) is related to a policy (chapter 2.2) that defines that rule. That policy is, in turn, a tool employed for governance (chapter 2.1). Several forms of governance are explored to examine how these produce policy and rules, as well as their usage of motivation as a stimulant for compliance. This desire for, and assumption of, perfect compliance will then be contrasted with the reality of non-compliance (chapter 2.4). Finally, motivational (chapter 2.5) factors for rule-breakers are covered. This information is foundational for the possible solutions (chapter 3) examined next.




Schematic depiction of the background chapters

The sections below follow a format in which a topic is first summarily introduced in relation to other sections and chapters, followed by an in-depth discussion of the topic itself. Finally, its content is briefly summarized for the reader's convenience.

## 2.1 Governance

To understand policy its origin must first be explored, which is governance. This provides insight into why policy is used, the influence (types of) governance has over policy, and its effects on those governed. To this end, various categories of governance will be explored. This basis is then further expanded upon in the policy section (chapter 2.2).

Although lacking a unifying theory [10, p. 1], governance can be broadly defined as "the pursuit of collective interests" [11, p. 3]. Traditionally, this is performed by a government that sets and steers society towards objectives, or coordinates economy sectors to ensure economic outcomes [12, pp. 134,136]. This pursuit has evolved over time and can be examined from various perspectives, resulting in different categorizations. The first categorization is "old" versus "new" governance and can be seen as an evolution in goals and approaches [13, p. 38]. Depending on employment of a rule- or risk-based approach, cybersecurity can be placed in either of these categories.

Old governance tends to be a hierarchical command-and-control structure which directs and monitors. It has a centralized form in which power resides in its own institutes, strictly dealing with public affairs. Its management style is rule-based, resulting in hard regulation based on a rigid belief system. Participation on policy is enacted through consultation, a form of tokenism, which is a participation level discussed later under Participation (chapter 3.1.1). New governance, in contrast, is polycentric in nature. It is a normative regime that federates its power to different actors that share information, resources, and results. One example is a participative nature preservation also covered in Participation (chapter 3.1.1). Its style of management is that of objective setting, resulting in soft regulation that relies on cooperation and alliances with other actors. Participation comes in the form of deliberation, involving indirect beneficiaries and breaking down decision process barriers.

Another categorization is governance either as a process or a structure [14, p. 5]. Governance as a process focusses on the outcomes of interactions between structures, instead of the structures them self, thus taking a new governance perspective. It expects objectives to change across sectors and over time, and thus their exertion of influences as well. However, one constant is the state structure that, given its control over critical resources, is still considered in a role of steering society as discussed earlier in this section. The other category is governance as a structure that is designed to address certain problems of governance and is formed either hierarchical, as a market, or a network.

The hierarchical structure is a bureaucracy that vertically integrates its institutes. The results in a top-down power structure in which subnational governments such as provincial institutes are always dependent on a centralized authority, thus making this old governance. When more autonomy is granted to these subnational institutes this is called multi-level governance, which in turn requires management of interaction between these levels. In this category direction to society is provided by bureaucracy through law and regulation, sometimes in consultation. However, the shortcoming of this structure is the assumption of total power held by the authority, such as the critical resources discussed earlier in this section. As this is no longer the case in modern society, where some power has shifted to large corporations, other structures of governance were created. The first generation of cybersecurity governance can be classified as hierarchical, embodied by a central security department that creates and enforces a rule-based information security policy about which its users are informed.

The market structure is an alternative approach, relinquishing exclusive control over critical resources and thus characterizable as new governance. It empowers citizens to determine which state services are offered and at what price, similar to economic markets, for example resulting in tax reductions. The state, in turn, focusses more on outcomes than means. To achieve its objectives it steers citizen behavior through market instruments such as incentives, instead of using coercive measures to discourage deviating behavior. This will be discussed in relation to Agency Theory, exemplified in an experimental study under Self-regulation (chapter 3.1.2). Power is increasingly decentralized through collaboration with private initiatives that sometimes extent into globalized markets, thus sometimes blurring the lines between nations. One of the shortcomings of this structure is that market forces can be driven by self-interest, inevitably diverging from the problems and needs of other actors.

The network structure is the final alternative. This joins public and private stakeholders together on a common interest, as demonstrated by the trade ban discussed in Policy (chapter 2.2). These stakeholders can include interest groups, state institutes, and industries from a policy sector. The cohesion between them varies, based on their common interest being either issue specific or related to

a policy. When issues are resolved networks can dissolve, but others last longer for larger policies. For national issues the state can assume the role of coordinator, relying more on soft regulation or new governance. Other issues can be industry specific, national, international, or even supranational, thus transcending coordination by an individual state. Within this alternative we find the next generation of cybersecurity governance, employing decentralized security departments operating on a risk-based information security policy created in consultation which its target audience.

All of these structures can exist in parallel but may conflict with one another. As such, governance of co-existing structures is required giving rise to meta-governance [15, p. 106]. While governance of cybersecurity has evolved to a new governance hands-off approach, there is also a tendency to regress back to an old governance hierarchical top-down command-and control model [16, p. 2].

In this chapter, governance has been defined as coordination and steering towards a collective interest. It can be categorized as old or new governance based on its goals and approach. Governance can also be seen as a process, focusing on results and interaction between actors, or as a structure. This structure can be hierarchical, with centralized institutions and hard regulation, such as classical rule-based cybersecurity governance. The market structure is centered on resource allocation which is softly regulation through market instruments. A network structure connects sectoral public and private stakeholders with softly regulated participation, for example more modern risk-based cybersecurity governance. Interaction between categories can be managed through multi-level and meta-governance. In the next section policy will be explored, and how it relates to governance, providing the basis for compliance (chapter 2.3).

## 2.2 Policy

Now that its origin is contextualized as governance (chapter 2.1), compliance (chapter 2.3) can be further explored through its point of reference, namely policy. This will provide insight into what policy aims to achieve, how it attempts to accomplish this, and what influences it. To this end, the source and creation of policy will be explored. This provides the underpinning for compliance (chapter 2.3), which will be covered afterwards.

The policy process can be defined as a “purposive course of action […] dealing with a problem or matter of concern” [17, p. 2]. A policy is always created in response to a demand from citizens, representatives, or public officials, such as covered later for local rulemaking and local monitoring (chapter 3.1.3). This demand in turn relates to a specific (public) issue, such as cartel forming or fatal accidents. Authorities, like legislators or corporate administrators, then craft and issue a policy statement addressing that issue. This statement can take the form of legislation, administrative rules, or even oral speeches. Examples can be condemnation of cartel forming in economic markets, backed up by punitive action, or health and safety regulation, as discussed later in the context of gamification (chapter 3.2.2). These are forms of positive statements that tackle the issue. Another course of action is a negative statement which purposefully chooses not to pursue the matter. Policies can also take on a coercive quality, such as backing by legal sanctions such as incarceration. Although private policies, such as organizational rules, can also incur (financial) consequences their legal standing is perhaps more dubious from a national legal perspective.

What is governed through policy? Organization theory recognizes the following interdependent variables, for example used in the network structure covered under Governance (chapter 2.1). Tasks are operations that satisfy an organizations reason of existence, such as production of goods. Actors refers not only to people, such as employees, but also legal entities like competitors and governments. Technology concerns technical tooling, for example a production line or computer systems. Structure consists of systems of authority, workflow, and communication [18, p. 55]. A popularized cybersecurity variant of these variables is people, process, and technology [19]. This variant has become an integral part of cybersecurity policies through industry standards [20] [21, p. 11], generally targeting one of these variables as exemplified later by alleviating people of Administrative burden (chapter 3.2.1).

The relation between policy and governance can perhaps best be demonstrated by the governance of cyberspace. This takes on the form of a network structure, both through its inherent networked technology as well as its transcendence of national borders. This network structure is also reflected in ensuing policy networks [22, p. 5]. Akin to multi-level governance policy must also account for horizontal relations between public and private actors and vertical relations between institutions [23, p. 27]. This leads to complex interactions, influences, and interdependencies, even for information security policies in a corporate context. An example of vertical influence is the representation of US trade interests. The US trade ban on foreign telecom equipment, allegedly used for industrial espionage [24], resulted in European regulation nudging member states into taking security measures, [25] and subsequently followed by national legislation shunning such equipment [26]. This policy mainly targets the technology variable. An example of horizontal influence is the regulatory spillover of the European General Data Protection Regulation (GDPR) outside of its territorial limits and policy domain [27]. This affects both the people and processes variables. These examples demonstrate policy is a powerful tool for steering the behaviors of actors towards collective interest but also influence a wide range of actors across different domains and (inter)national borders, who themselves may not be pursuing the same interests.

This chapter defined policy as a course of action dealing with a matter of concern and created in response to a demand. Its nature can be coercive through sanctions, and it targets either people, process, or technology. Governance of cyberspace is rooted in new governance, which is reflected in the ensuing policy networks. Subsequent policy can exert influence both horizontally and vertically, affecting a variety of actors. In the next section, compliance and its relation to policy will be explored, providing context for non-compliance (chapter 2.4).

## 2.3 Compliance

Now that it is identified that rules originate from policy (chapter 2.2) and governance (chapter 2.1), the expectation of adherence to those rules will be explored. This will provide insight into why (cybersecurity) policy is (in)effective, and what may be the basis for this. To this end, compliance will be explored, as well as the means to stimulate this. This provides a frame of reference for the upcoming distinction with non-compliance (chapter 2.4).

Compliance is defined as “the act of obeying a law or rule” [28], such as stipulated by a cybersecurity policy. This is a tool that can be used for the concept of steering and coordination discussed under Governance (chapter 2.1), with the goal to stimulate citizens or employees to follow the rules set out by policy. To encourage obedience policy usually has a coercive quality. That quality not

only comes from its authoritative source, such as legislators or corporate policy writers, but also from the threat of sanctions, like punishment. This concept of rules and punishment originates from General Deterrence Theory (GDT) and is based on the premise that (severe) punishment will dissuade further rule breaking (by others) [29, p. 128]. Research is divided on its effectiveness. One side argues that punishment certainty is the main deterrent for crimes [30, p. 124]. The other claims there is a great discrepancy between its claims and actual effects, even going so far as to state non-legal factors are more effective [31, p. 765]. Nevertheless, GDT is widely adopted. Examples include sanctions in international law, prison sentences in criminal law, fines and dischargement in contract law, and punitive action as covered in Agency Theory under Self-regulation (chapter 3.1.2). As such, it is perhaps unsurprising deterrence techniques are also employed for cybersecurity, and industry standards require disciplinary action in response to employee misconduct [32, p. 11] [33, p. 85].

In this chapter compliance has been defined as the act of obeying rules from policy (chapter 2.2). Deterrence, or punishment, was identified to be widely adopted to stimulate this, even though its effectiveness is called into question. Finally, the application of deterrence within cybersecurity is touched upon. The next section covers non-compliance, providing insight into the motivation (chapter 2.5) factors discussed afterwards.

## 2.4 Non-compliance

Now that compliance (chapter 2.3) with policy (chapter 2.2) rules has been explored, the act of disobedience to those rules can be examined. This provides insight into why misconduct occurs, thus changing the perspective on its root cause. The motivation (chapter 2.5) for compliance and non-compliance are examined afterwards.

Employees are considered to be one of the biggest threats to cybersecurity [34, p. 8] [35, p. 8]. They are widely regarded to be the Achilles' heel of cybersecurity, referred to as an 'insider threat' causing incidents through deliberate actions or neglect, explaining the apparent need to govern employees through cybersecurity policies. Deliberate actions are commonly attributed to a "disgruntled employee or espionage" [9, p. 102], exemplified by the US trade ban discussed under Policy (chapter 2.2). Neglect is said to be introduced through "passive noncompliance with security policies, laziness, sloppiness, poor training, or lack of motivation" [9, p. 102]. This sparked much scientific interest into non-compliance with cybersecurity policies, resulting in a great amount of scientific research yielding many scientific papers. Surprisingly, although the majority of this research implicitly relates cyber incidents to policy violations, evidence for this supposed causality remains scarce. However, (deliberate) non-compliance with cybersecurity policies has been proven to exist. In healthcare it was observed "when an emergency alarm sounded, nurses [left] the computer logged on with the medical record on the screen", which was "a non-compliant action" even though "hospital staff were aware of the rule" [36, p. 50]. Additionally, employees self-reported "failing to fully adhere to cybersecurity policies at least once", with "an average failure-to-comply rate of once out of every 20 job tasks" [37].

This chapter detailed perceptions pertaining non-compliance with cybersecurity policy (chapter 2.2) surrounding employees. Additionally, it demonstrated the interactions between governance (chapter 2.1), policy, and the various actors in a network structure. Finally, it noted that non-compliance does indeed exist. The next section will examine motivation factors of non-compliance, later used for finding possible solutions (chapter 3).

## 2.5 Motivation

After exploring non-compliance (chapter 2.4) and policy (chapter 2.2), the motivation behind this can be explored. This will provide insight into the cause of non-compliance and may provide direction for remediation to increase compliance (chapter 2.3). To this end, types of motivation, and their contributing factors, will be explored.

Motivation is defined as the "enthusiasm for doing something" [38]. Self-Determination Theory (SDT) distinguishes between two types of such enthusiasm. Intrinsic motivation is "the innate, natural propensity to engage one's interests and exercise one's capacities" which a person does "for internal rewards such as interest and mastery" [39, pp. 43,49]. When possible people will exhibit this inherent quality, although environmental factors such as social circumstances can interfere with its manifestation. One approach to stimulate this enthusiasm is discussed later in Gamification (chapter 3.2.2). A sub-theory of SDT, Cognitive Evaluation Theory (CET) [39, p. 62], identifies the three contributing aspects to intrinsic motivation as autonomy, competence, and relatedness. Autonomy is the extent to which one can determine one's own behavior, which in turn enhances intrinsic motivation. This is also part of Self-regulation (chapter 3.1.2). Competence is an intrinsic need for mastery, which is usually increased when a person succeeds or gets positive feedback. Relatedness is the feeling of connection with others, of belonging (to a group), which plays a role in Participation (chapter 3.1.1). Extrinsic motivation, in contrast, refers to "behavior where the reason for doing it is something other than an interest in the activity itself" which a person does "to get an extrinsic reward or to comply with an external constraint" [39, pp. 35,49]. Such behavior can however be something a person feels pressured to do. This enthusiasm is commonly stimulated either through incentives, like rewards, or deterrents, such as (fear of) punishment. As discussed in Motivation (chapter 2.5), deterrents are used by General Deterrence Theory, and commonly employed in information security policy (ISP).

Although widely used, the positive effects of extrinsic motivation are contested, in part demonstrated through the existence of Non-compliance (chapter 2.4). Some studies favor rewards, stating "there is […] good evidence that rewards have a strong influence on the students' motivation" [40, p. 456]. Others lean towards punishment, claiming policy misuse is deterred "primarily by increasing users' perceptions of punishment severity" as well as the perception of being caught [41, p. 162]. A third movement is more uncertain, warning that "while reward systems can generate the same positive effects as punishment systems, they also generate the same negative side effects" [42, p. 253]. However, the majority of studies conclude extrinsic motivation to be either ineffective, stating "Motivation driven by a desire to obtain rewards or avoid punishment (external regulation) was not associated with performance" [43, p. 1300], or even yielding a negative effect, warning that "the undermining of intrinsic motivation by tangible rewards is indeed a significant issue" [44, p. 15]. In contrast, intrinsic motivation has been found to have a more positive effect on compliance. For example, "extrinsic motivation […] in clinical encounters ha[s] no significant relationship on [...] compliance" while "patient compliance is largely driven by autonomous regulation as proposed by SDT" [45, p. 453], where autonomy is a contributing aspect to CET. Similarly, and specifically in relation to ISPs, "variables rooted in the intrinsic motivation model contributed significantly more to the explained variance of employees' compliance than did those rooted in the extrinsic motivation model" [46, p. 296]. The latter can be related specifically to CET, as "perceived autonomy, perceived competence, and perceived relatedness significantly predicted security policy compliant behavior" [47, p. iii], which are contributing aspects to CET.

In this chapter motivation has been defined as enthusiasm for doing something. This can be divided into intrinsic motivation, coming from within, and extrinsic motivation, coming from without. Additionally, the effectiveness of stimulants for extrinsic motivation, incentives and deterrents, have shown to be mostly ineffective or negative. Intrinsic motivation, specifically the contributing aspects autonomy, competence, and relatedness, was shown to have a positive effect on ISP compliance. In the next chapter possible solutions are explored and correlated with the foundation laid out in this chapter.

# 3 Possible solutions

After identifying the positive effect of intrinsic motivation (chapter 2.5) on compliance (chapter 2.3), and an ineffective or negative effect of deterrence as an extrinsic motivation, solutions from other domains are explored. These are examined for possible application to cybersecurity, and the feasibility thereof, in accordance with the Methodology (chapter 1.2). The results are grouped in categories based on thematic commonalities, providing a potential direction for solutions, and summarized as follows:

| Category | Solution | Brief description |
|---|---|---|
| Governance | Participation | Users collaborate on rule creation |
| | Self-regulation | Users create rules |
| | Local rulemaking and monitoring | Users create rules and monitor adherence |
| Policy | Administrative burden | Reduce users' overhead induced by rules |
| | Gamification | Increase rule adherence through game elements |
| Communication | Framing | Increase rule adherence by changing users' perception |
| | Motivational interviewing | Increase rule adherence by using users' own values |
| | Prosocial motivation | Increase rule adherence by increasing users' empathy |
| | Autonomy-Supportive behavior | Increase rule adherence by increasing users autonomy |
| Education | Bias correction | Increase rule adherence by correcting faulty perceptions |
| | Awareness training | Increase rule adherence through training |

Overview of the categorized possible solutions along with a brief description.

The following sections follow a format in which possible solutions are grouped together according to their solution direction, related to the previously examined Background (chapter 2), and briefly summarized. Individual sections then first introduce the theoretical framework underpinning the approach, after which a number of cases are detailed.

## 3.1 Governance

As the relationship between policy (chapter 2.2) and governance (chapter 2.1) has been identified the possibility of influencing compliance (chapter 2.3) with policy through governance can be explored. Participation (chapter 3.1.1) in nature preservation is implemented through decentralization, and an experimental setting shows potential benefits of cooperation. These topics will also be revisited for local rulemaking and local monitoring (chapter 3.1.3), administrative burden (chapter 3.2.1), and gamification (chapter 3.2.2). Self-regulation (chapter 3.1.2) in technology uncovers the power of justice beliefs, with similar results for values in defense and law enforcement. Finally, local rulemaking and monitoring (chapter 3.1.3) in nature preservation is shown to have potential positive effects on motivation (chapter 2.5).

### 3.1.1 Participation

Participation within companies is defined as "human collaboration in the organizational setting" [48, p. 48] by Theory Y, which stipulates people seek self-direction, self-control, and responsibility for organizational objectives. The level of participation can be plotted on a "range of managerial actions" related to decision and implementation. Negligible participation results from a manager hosting a conversation to inform subordinates and provides an opportunity for questions. Participation increases when a discussion is held about implementation, or prior to the decision. Finally, a superior may discuss the issue beforehand, or accept any decision from subordinates [48, p. 126]. Another view is "levels of participation" [49, p. 217]. Non-participation aims to persuade participants of their contrary view

through manipulation or therapy. Tokenism allows participants to hear and be heard, by informing, consultation, or advisement, but does not grant them any power. This is often seen in old governance hierarchical structures. Citizen power is achieved through partnership, allowing for negotiation, delegation, or empowered citizens through majority or full managerial power. These degrees can be seen in new governance, such as the market and network structure. Full managerial power is synonymous to autonomy, which is also one of the contributing aspects of Cognitive evaluation theory (CET).

Within nature preservation a field survey indicates that "decisions to violate management regulations [...] related to [...] fishermen's participation in their organizations", and is influenced by social aspects such as "the level of legitimacy of the norms and the sense of belonging" [50, p. 271]. This result stems from a management system that integrates rights and responsibilities of local users of the preservation in decision making. A Participatory Management Board has been instituted which involves local fisherman in proposals regarding fishery activities. These are then submitted to a Management Authority resulting in legislation. This is a new governance approach, in part multi-level governance, and a network structure through partnership. The sense of belonging is synonymous to relatedness, one of the contributing aspects of CET. In cyberspace this approached can be duplicated by establishing a Cybersecurity Management Board in which employees partake. As with every form of direct democracy, a question of scale arises given the average number of employees in a company. This can be addressed by implementing a representative model, safeguarding the interests of employee groups regardless of size. Additionally, the extend of the boards' decision-making power should be clearly defined.

A university experiment showed "participatory decision making and enforcement, influence voluntary cooperation", the latter which was operationalized "as percentage rule compliance" due to "perceptions of [...] self-determination" such as competence [51, pp. 511,517], one of the contributing aspects of CET. In a common-pool resource simulation group participants collected resources to earn money based on a ruleset determined democratically beforehand, the result of which were shared with the group after this process. Group members could then impose sanctions for (supposed) rule violations reducing money earned for other members, which the entire group was again informed about. This approach is a mix of new governance, a decentralized market structure, and old governance, not so much with command as through mutual influence (over group members). Application to cybersecurity is questionable due to the assumption of a 'shared resource'. Where the simulation participants had a common financial interest, a cybersecurity interest may not be equally prevalent across employees. Equalizing this intangible value would require additional stimulants. Also, the punitive aspects related to General Deterrence Theory (GDT) have been questioned repeatedly by other research (see chapter 2.3), even though its effects were positive in this research. Finally, the potential pitfalls of the prior nature preservation field survey are equally applicable here and should be addresses similarly.

### 3.1.2 Self-regulation

Agency Theory defines self-regulation as "overriding one response or behavior and replacing it with a less common but more desired response" which "enables people to alter their behavior so as to conform to rules" [52, pp. 2,5]. Here, a principle (e.g. the government) in essence delegates regulation to an agent (e.g.: a company or industry) instead of directly applying regulation. This can be characterized as new governance, although perhaps with the shadow of authority. Divergence from the

principle's interests can be limited by providing incentives or incurring costs [53, p. 308], which is remnant of old governance relying on GDT.

Within technology an online survey determined a "self-regulatory strategy is a viable approach to attaining rule adherence" and noted intention to comply is motivated by "organizational justice beliefs and personal ethics" [54, pp. 493,497], where self-regulation signals a new governance approach. The survey instrument measured the constructs personal ethics, organizational justice belief, procedural justice, distributive justice, interpersonal justice, informational justice, and intention to comply related to these results. Personal ethics reflect (judgment of) moral values. Organizational justice belief is divided into four dimensions, procedural, distributive, interpersonal, and informational. Procedural justice is the perceived fairness of procedures. Distributive justice is about the fairness of outcomes of oneself in relation to others. Interpersonal justice pertains the conduct of enforcers, such as respectfulness and politeness. Informational justice is about authorities sharing information about process and outcome. Finally, intention to comply relates to gender, age, internet experience, and company monitoring practices. Within cybersecurity these constructs could to some extent be implemented. Personal ethics cannot, and probably should not, be influenced directly, as this level of influence of employees by employers could be an unethical intrusion on their private life. What might be approximated is alignment between corporate and personal values, to the extent that this is possible with a large group number of employees. This could be achieved by adjusting corporate values in relation to personal values, for example based on employee surveys of interviews. Another approach can be a hiring strategy that performs screening, although this would impact diversity and could be a legally questionable form of discrimination. Procedural justice could be achieved by introducing transparency about processes as well as the reasoning behind it. The latter aims to foster understanding in employees. It also provides a basis for conversations and discussions, such as those of rule revisions and deviations. Distributive justice requires standardization. Commonly, (the type of) sanctions are often at the discretion of managers, thus (unknowingly) introducing a degree of unfairness. Standardization could be implemented in the form of a playbook, perhaps augmented with registration. The latter comes with privacy challenges and is also unnecessary when managers can be trusted to 'play by the book'. Interpersonal justice could be achieved through interpersonal training to develop soft skills. The challenge is that technical skills, as cybersecurity is still dominated by technical people, don't always go hand-in-hand with communication skills. Additionally, (technical) cybersecurity operations could be segregating from security officers, the latter handling 'customer contact'. Informational justice could be obtained by wide distribution of cybersecurity policies through different channels, both digital (such as intranets, internal social media, etc.) as well as through personal contact, such as trainings.

A survey in defense and law enforcement found that "encouraging selfregulation via appeals to the values [...] is a viable strategy for minimizing misconduct" [55, p. 457]. The results show those values were mostly shaped by procedural justice, which in turn was primarily influenced by justice of organizational decision-making and justice of interpersonal treatment by one's superior [55, p. 478]. This is a new governance approach, of which the specific constructs [55, p. 487] underlying these elements could be applied to cybersecurity. Organizational decision-making requires rules are applied equal, fair, factual, and transparent. Equality could be achieved by standardization of both rules and procedures, which can additionally employ centralized monitoring and enforcement, although this could introduce a degree of impersonality. Fairness requires cybersecurity policy is written with proportionality in mind, both in its rules as well as any consequences of non-compliance. Factuality requires monitoring to

gather the facts, which could be augmented by 'organizational distance' that introduces a degree of impersonality to decrease emotional bias. Transparency could be obtained by wide distribution of cybersecurity policies through different channels, both digital (such as intranets, internal social media, etc.) and through personal contact, such as trainings. Interpersonal treatment requires attention, consideration, trust, and respect. Interpersonal training could target all of these. Attention requires listening to employees' views on matters and issues. Consideration is taking into account those views in design and processes. Trust could be fostered by demonstrating reliability, for example by implementation of those views when the situation permits this. Respect is accepting the views in a fashion that leaves the dignifying of employees intact.

### 3.1.3 Local rulemaking and monitoring

Local rulemaking aims to address local needs by relinquishing centralized power to local entities. This can be a "local rulemaking authority" granted "the ability to address local procedural needs" [56, p. 484] or governments "beginning to push ownership and control of public services [...] into communities" [57, p. 53]. Local monitoring (of compliance) can be implemented in various categories of a monitoring topology. One end is "externally driven, professionally executed", or non-localized, which is old governance. The other end is "autonomous local monitoring", or fully localized [58, p. 33], which is new governance. The latter is synonymous to autonomy, which is one of the contributing aspects of CET.

A nature preservation study based on an existing database suggests that compliance is more likely "when local rulemaking is combined with local monitoring" which "might actually enhance intrinsic motivation" [59, pp. 312,313]. The following variables were used in the study's models. Local rulemaking represents whether (earlier generations of) local groups created operational rules. Local monitoring constitutes whether group members regularly organize monitoring. Some additional variables were included. Collective action index represents member collaboration unrelated to the forest. Poor relates to poverty levels. Density represents the number of households. Other group signifies activity by other groups. Market measures the physical distance to the nearest market. These are extended with the control variables commercial users, commercial value, and external monitoring. This is a new governance approach. Cybersecurity application of local rulemaking would be similar to that of self-regulation (chapter 3.1.2). Local monitoring could to some extend be applied. Care should be taken to retain the three lines of defense, preventing employees who are non-compliant to hide their own actions. For this, a four-eyes principle could be instituted, although favoritism among colleagues could pose a similar challenge. Both issues could be solved by a tiered model, where local monitoring is performed, but audited independently periodically.

Another nature preservation study using data from the same database states success depends on "institutional arrangements that (1) establish local resident rulemaking autonomy" and "facilitate […] institutional assistance for monitoring and enforcement of local rules" [60, p. 545]. The following topology of five property rights [61, p. 251] were scored on the extent to which they were held solely by local forest users, jointly with a government authority, or only by a government authority. Depending on that extend this is either old or new governance. Access is the right to access the forest. Withdrawal means the right to obtain resources from the forest. Management represents the right to regulate the forest. Exclusion stands for the right to determine access to the forest. Alienation is the right to sell or lease out the forest. In cybersecurity, this codification of measurement variables is difficult to translate to a practical intervention. Management represents the level of participation of employees and can be

applied to cybersecurity as noted earlier. The other rights can be seen as universal to cyberspace, at least in a corporate environment. With difficulty these could be shoehorned, for example exclusion to Identity and Access Management, but would represent a specific aspect of participation that doesn't require that level of detail.

## 3.2 Policy

As the relationship between compliance (chapter 2.3) with rules from policy (chapter 2.2) has been identified, the possibility of influencing compliance (chapter 2.3) through policy changes can be explored. Administrative burden (chapter 3.2.1) in law enforcement is demonstrable related to participation (chapter 3.1.1), similarly affecting motivation (chapter 2.5) in agriculture. Additionally, gamification (chapter 3.2.2) in both healthcare and safety shows an effect on compliance can be generated.

### 3.2.1 Administrative burden

Administrative burden is "a function of learning, psychological, and compliance costs" due to "interactions with government [62, p. 43]. It "arise[s] from engaging in search processes to collect information", includes "the stigma of [...] participating in a program with negative perceptions", a "sense of loss of [...] autonomy", and are "the burdens of following administrative rules" [62, p. 45].

In law enforcement an experiment showed that "reducing friction costs to participation and simplifying processes" improved compliance [63, pp. 98,99]. During the second phase of a recruitment process the application could be performed online instead of in-person, significantly reducing the lead time. Additionally, the content of official email communications was reduced in length by half, and reminders were sent out via text messages. This could be incorporated into cybersecurity. Processes, such as audits, could be largely automated online, including communication surrounding this. While digital processes are not new to the cybersecurity domain, compliance can be slightly more old-fashioned and be limited to digitization of forms that need to be filled in and send out manually. A pitfall is fully automated processes being prone to becoming impersonal, which could be remediated through a hybrid approach where human guidance is still available and provided. Additionally, the content of cybersecurity policies could be more condensed, while retaining their essence, to decrease time consumption and increase accessibility.

In agriculture a survey noted a "strong positive effect of compliance costs on administrative burden" was found and "farmers perceive a loss of autonomy because of […] policy" which "might negatively affect their perceived administrative burden" [64, pp. 4,13]. Compliance costs measurement was based on three items. Change in administrative workload, time spend on documents, and time spend on inspections. This could be implemented in cybersecurity through automation, which could address all these issues. Administrative workload and documentation time could be decreased by automatic data retrieval. Additionally, automatic submission could be added, although this might touch on issues regarding privacy and legality. Inspections could also be automated to some extent, although this would require impartial information gathering and validation which can be problematic in a digital environment. Naturally, such automation should be implemented with cybersecurity in mind.

### 3.2.2 Gamification

Gamification stipulates once employees "are sold on the value of scorekeeping and their personal goals are consistent with the overall goals of the company, the rules are clearly defined, and

results to resource ratios are in place, allowing the people to know if they are winning or losing every day, their increased productivity will be phenomenal. Being sold is the key, and choice makes the difference" [65, p. 141]. The alignment of personal and company goals can be characterized as relatedness, one of the contributing aspects of Cognitive evaluation theory (CET).

An experiment in healthcare found "the use of gamification incentives was associated with an improvement in the frequency of blood glucose monitoring" [66, p. 10]. A mobile application was developed to gamify management tasks for patients with diabetes. Points were awareded for each (consecutive) glucose reading, with bonuspoints awarded for a full day of readings. A set amount of these points could be redeemed in the mobile app store for purchases [66, p. 6]. In cybersecurity points could be associated with secure behavior, for example performing security tests on products or reporting phishing mails. These points could be linked to monetairy incentives by providing more budget for projects, or reducing the price of a lunch.

A field experiment in safety noted gamification resulted in "better adherence to project rules and policies" [67, p. 819]. A game was created that incorporates a point system, a leaderboard, feedbacks loop, and a cash price [67, pp. 806,811]. Points were awarded when achieving a small goal and compared between construction workers. The top three employees were offered a cash price by their manager. In cybersecurity the concepts of points and leaderboards can be applied to secure behavior by employees. Care should be taken the leaderboard is not in essence a wall-of-shame for trailing scores or non-participation. As cash prices are also used as performance incentives within corporate environments, through a bonus, secure behavior could also be classified as a performance indicator and incentivized likewise.

## 3.3 Communication

Naturally, compliance (chapter 2.3) requires awareness of the (reasons for) existence of policy (chapter 2.2). Styles and types of communication pertaining this existence and policy content are examined. Framing (chapter 3.3.1) in both retail and an experimental setting demonstrates how phrasing can affect compliance. Motivational interviewing (chapter 3.3.2) in healthcare is discovered to affect adherence, and it is hypothesized this technique can affect motivation (chapter 2.5). Prosocial motivation (chapter 3.3.3) is shown to affect compliance, and a healthcare experiment demonstrates tiny changes can yield big results. Also, autonomy-supportive behavior (chapter 3.3.4) can be influenced by auditors in health and safety and was found to change perspectives in healthcare.

### 3.3.1 Framing

Framing can be split into frames in communication and frames in thought. Frames in communication refers to "the terms to refer to the words, images, phrases, and presentation styles that a speaker uses", while frames in thought refers to "an individual's (cognitive) understanding of a given situation" [68, pp. 227,228]. Frames in communication can in turn be split into frame building, "the processes that influence the creation or changes of frames", and frame setting, regarding "salience [...] and perceived importance of frames" [69, pp. 115,116].

A survey in retail regarding "differences between the Fine and Deposit programs" found "the Deposit program was perceived not only as more desirable but also as more effective" [70, p. 431]. The following regulatory mechanisms were compared. Deposit returned money to the consumer after returning bottles at recycling points. Fine imposed a monetary penalty equal to the deposit for

discarding bottles in normal waste bins. Ethical Code appealed to an environmental ethical code. Employing incentives is a market instrument of the new governance market structure. In cybersecurity policy could be rewritten to reframe cybersecurity as a quality aspect instead of incurred costs. For example, costs for security measures and audits could be considered an investment in better products and services, instead of a penalty for non-compliance.

Experiments in a university concluded that "If the available incentive is framed as a bonus [...] voluntary cooperation is [...] significantly higher than in a situation in which the incentive is framed as a price deduction" [71, p. 31]. The incentive experiment consistent of buyers and sellers attempting to agree on a contract. Buyers first offer a contract detailing price and quality. Sellers can then accept one of the contracts. After accepting, sellers choose their quality level, regardless of the quality specified in the contract. Buyers can then punish sellers if quality can be proven to fall short. Additionally, the bonus experiment reframed the fine as a bonus, not to be paid in case quality can be disproven. For cybersecurity the same comments and solution direction(s) from the retail survey above are applicable.

### 3.3.2 Motivational interviewing

Motivational interviewing is "about arranging conversations so that people talk themselves into change, based on their own values and interests" and lives in "this middle ground [along a conversation continuum] between directing and following, incorporating aspects of each" [72, pp. 4,5].

In a healthcare experiment motivational interviewing "has been used effectively to change a number of health-related behaviors" in order "to raise patients' awareness of their thoughts/feelings about adherence" [73, pp. 42,43]. Patients received a twenty-minute audiotape and a booklet, two one-on-one sessions, and two mailing after two weeks. The session focused on concerns the patient deems salient, during which the counselor employs techniques like reflective listening and issue reframing (see chapter 3.3.1) to raise awareness of thoughts and feelings about adherence. This approach does not seem viable for cybersecurity in a corporate environment. A logical candidate for one-on-one sessions would be superiors, who often lack adequate cybersecurity knowledge. Another option is decentralized security specialists, such as security officers. Group sessions could be an alternative, although this would likely yield suboptimal results because directing and following conversations will prove complex when values and interests of participants inevitably divert. All options would require specialized training, likely relying on prior therapeutic or counseling experience. The audiotape, booklet and mailings could be integrated in education, although they seem secondary to this approach.

A hypothesis at a university states motivational interviewing may "also provide a useful application of SDT's concept of autonomy-support" [74, p. 76], an approach which will be discussed further in Autonomy-Supportive behavior (chapter 3.3.4). An integrated theory of self-determination theory (SDT) and Motivational Interviewing (MI) is proposed. Fostering change can be achieved by mutual agenda setting, reflective listening and summarizing. Mutual agenda setting from MI ensures clients' concerns and goals are reflected, consistent with autonomy support from SDT. Reflective listening involves repetition of words verbatim or emphasized, to help increase self-awareness of thoughts and feelings, improving a persons' position to make autonomous choices. Summarizing is used to link together the discussed material, again helping to increase awareness. In Cybersecurity, some of these techniques can be applied. Mutual agenda setting can be used directly with employees or within teams, for example regarding project goals or strategic plans. Reflective listening and summarizing concern soft skills, which can be used in contact between cybersecurity personnel and employees, for

example during trainings. The latter is probably harder to implement, as this would require specialized interpersonal skills most likely relying on pre-existing (specialized) communication skills.

### 3.3.3 Prosocial motivation

Prosocial motivation is “empathy, defined […] as an affective response that is more appropriate to someone else's situation than to one's own” [75, p. 281], and “is egoistic when the ultimate goal is to increase one’s own welfare; it is altruistic when the ultimate goal is to increase another’s welfare” [76, p. 67]. When it is altruistic this requires measure of relatedness, which is a contributing aspect of CET.

A survey across multiple domains found prosocial motivation to “positively affect voluntary […] compliance behavior”, while giving caution of “the negative effects of instrumental controls (e.g., deterrence) on such behaviors” [77, p. 1]. Prosocial motivation consists of perceived prosocial impact and perspective taking. Perceived prosocial impact concerns individuals’ recognition of impact of their actions on clients. It measures the extent to which individuals’ want to make a difference, help, have a positive impact, and to do good. Perspective taking is the extent to which individuals can adopt clients’ viewpoints. It measures the extent to which individuals’ take clients’ perspectives, imagen how clients feel, make an effort, and seek to understand clients’ viewpoints. Instrumental controls are measures for regulation of organizational policy conformity. It measures the extent to which policy rules and processes adherence is required and enforced. This could be applied to cybersecurity. Perceived prosocial impact could be fostered through training and demonstrating the positive effects of employee conduct and actions on (clients’) cybersecurity, for example showing it can stop attacks or reduce their impact. Perspective taking can be fostered through client contact, introducing cybersecurity personnel to employees, and facilitate conversations and discussions to gain insight. The negative impact of instrumental controls could be reduced through reframing their imposed nature and being transparent about their reasoning to foster understanding.

Field experiments in healthcare found “hand hygiene of health care professionals increased significantly when they were reminded of the implications for patients” [78, p. 1494]. The behavior of healthcare professionals was compared based on virtually identical signs, emphasizing personal consequences or patient consequences, by changing a single word. In cybersecurity this could be applied in formulation of policy and training content, where consequences of security behavior and issues are related to co-workers or customers.

### 3.3.4 Autonomy-Supportive Behavior

Cognitive evaluation theory (CET) states that “events that lead to an internal perceived locus of causality and enhance intrinsic motivation [...] support autonomy”, further defining “The perceived locus of causality” as “a cognitive construct representing the degree to which one is self-determining” [39, p. 62].

A survey in health and safety determined that “Relative to coercive inspectors, autonomy-supportive inspectors [...] achieved compliance after fewer worksite visits” [79, p. 271]. For less serious violations, inspectors could use their own discretion for issuing either a voluntary or formal compliance order. They were also free to determine the number of compliance orders as well as the amount of follow-up inspections. Results show autonomy-supportive inspectors used less severe compliance orders and utilized the compliance process as an opportunity to educate about compliance, rather than using coercive methods. Applying this approach to cybersecurity can work to some extent. The approach to

internal compliance and audit processes can be one of support, providing more freedom and leeway, instead of the usual coercive approach. However, this becomes more challenging for externally driven compliance, where a 'soft' approach could be used but (timelines for) requirements are not flexible, thus incurring legal and financial risks.

A survey in healthcare determined "autonomous motivation was found to relate to perceptions of the physicians' autonomy support" [80, p. 274]. Physicians' autonomy support was measured for the following items [81]. Choice and options being offered by physician. Feeling understood by physician. Ability of being open to physician. Physician conveying confidence of patient abilities. Acceptance by physician. Physician ensuring comprehension of condition. Physician encouragement for questions. Feeling trust in physician. Physician listening for action course. Physicians' handling of emotions. Physician caring about patient. Physician interaction style. Physicians' attempts at understanding patient views. Patients' ability to share feelings. In cybersecurity these items could be applied, and are mostly related to soft skills. Choice and options could be integrated in a risk-based approach by providing alternatives and leaving final decisions to employees. This is, most likely, best implemented in a hybrid approach, where some decisions are still driven by rules for external compliance (also see the previous survey). Closer collaboration by cybersecurity personnel could foster understanding of the situation and reasoning of employees, addressing feeling understood, acceptance, condition comprehension, encouragement for questions, and understanding employee views. This could be augmented with interpersonal training, which addresses handling of emotions, conveying confidence, acceptance, caring, and interaction style. Finally, trust can be instilled by cybersecurity personnel through operationalizing input from employees, addressing ability of being open, feeling trust, and ability to share feelings.

## 3.4 Education

Awareness of policy (chapter 2.2) is not enough for compliance (chapter 2.3), as its content needs to be consumed as well. Education is one of the approaches to achieve this. Bias correction (chapter 3.4.1) in technology shows perception is related to adherence, while psychology shows perceptions of oneself also plays an important role. Additionally, Awareness training (chapter 3.4.2) in the maritime industry demonstrates the relation between training and performance, while a university training also shows its influence on behavior.

### 3.4.1 Bias correction

Cognitive biases "stem from the reliance on judgmental heuristics". Three heuristics are used in uncertain conditions. Representativeness is "usually employed when people are asked to judge [...] probability". Availability is "often employed when people are asked to assess [..] frequency [...] or [...] plausibility". Adjustment from an anchor "is usually employed in numerical prediction when a relevant value is available" [82, p. 1131].

Questionnaires in technology found "Providing accurate information on the amount of wrongdoing should reduce the bias and diminish wrongdoing" [83, p. 907]. People were asked if they would divulge trade secrets. Additionally, they were asked to estimate how often colleagues would do the same, and how frequently employees in their region would do so. Colleagues were estimated more likely than people themselves, in turn surmounted by employees in their region. In cybersecurity this bias could be corrected by providing accurate (real-time) information on cybersecurity issues, such as

active exploitation of vulnerabilities, the amount of data leaked in a security incident, and financial consequences for the company.

Questionnaires in psychology determined “A pervasive tendency was found for subjects to associate themselves with fair behaviors and others with unfair behaviors” and “behaviors that began with ‘I’ were rated as significantly fairer than those that began with ‘They.’” [84, pp. 480,487]. Subjects were given two assignments. One requested to list unfair behaviors while the other asked for fair behaviors. The fair and unfair results where then categorized according to the usage of ‘I’ and ‘they’. In cybersecurity this can be applied by designing which personal pronoun is used in policies and trainings, for example by priming questions such as ‘what would you do if…’, more likely prompting ‘I would than do…’ answers. Careful consideration should be given to a shift in pronoun usage since the referenced study: where ‘they’ previously referred solely to a group of other people, this can now also refer to a singular person of unspecified gender.

### 3.4.2 Awareness training

Security awareness is “the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly” [85, p. 6]. It was used in the “Careless Talk” campaign during World War II to reduce leaks “about troop-movements and convoy sailings” [86, p. 91] and consists of three dimensions: “what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour)” [87, p. 291].

A survey in maritime industry found that “When security awareness is increased by effective security training, an enhanced security performance [on]board is achieved and this reduces the likelihood of occurrence of security threats” [88, p. 210]. The security training items that were measured were as follows. Training importance, practical use, course satisfaction, security awareness contribution, and action implementation contribution [88, p. 206]. In cybersecurity these items can be incorporated into (existing) awareness trainings. Importance could be demonstrated through (practical) examples of policy violations, including consequences for colleagues or the company. However, this does rely on a level of transparency regarding security breaches that is not yet common in the industry. Practical use, action implementation, and course satisfaction could be achieved by tailoring to employee context, such as a specific processes or certain technology. As tailoring to individual employees likely incurs disproportional costs, given the average amount of employees in companies, group tailoring might be preferable. Security awareness contribution could be achieved by aligning training with policy, which should incorporate the previously mentioned items.

A post-training questionnaire at a university found that a “training session had a positive effect on employees’ security knowledge and attitudes towards security” and “The impact of the training on staff members’ self-reported behaviour was also found to be positive” [89, pp. 11,12]. Security knowledge was measured through understanding the difference between fire alarms and bomb alerts, where to report suspicious behaviors and crimes, and where to go with questions. Security attitudes was measured via sentiments towards the importance of security, reporting of suspicious behaviors and situations, and responsibilities for security. Self-reported behaviour was measured through conduct towards reporting noticing suspicious persons, falling victim to a crime, and experiencing an emergency. In cybersecurity these items could be incorporated into (existing) awareness trainings. Security knowledge can be increased by explaining about various cyber incidents, such as a data breach or denial

of service. Additionally, contact details of cybersecurity departments, with their respective responsibilities, could be distributed through various communication channels, including posters. Security attitudes could be increased by teaching about the impact of breaches of security on the company as well as employees, and how to reduce or prevent them by reporting suspicious situations. Additionally, security responsibilities could be explained to be owned by all employees, and not just cybersecurity departments. Role playing could be instrumental in measuring the effects of this. Self-reporting could be bolstered through simulations and being transparent about contributions of employees surround security issues. The latter could also be anonymized for privacy reasons.

# 4 Discussion

For some people compliance (chapter 2.3) with cybersecurity policy (chapter 2.2) is the silver bullet that will put an end to cybersecurity incidents. Whether this is true or not, there seems to be an inherent flaw in the approach that aims to achieve this, given the proliferation of cybersecurity incidents. For many years the focus has been lack of knowledge of employees, thus attempts were made to remediate this through security awareness training [8, p. 757]. But surely, this 'knowledge gap' must have been closed by now through all those trainings. This research attempts to shift this focus on knowledge towards that of motivation (chapter 2.5) through a literature review of compliance within other domains, and what alternative approach are used to achieve this.

The use of extrinsic motivation to stimulate adherence is so commonplace it hardly requires further explanation. We are all familiar with punitive deterrents, such as traffic fines, and financial incentives such as a bonus are not uncommon. As such, it is interesting to find the use of intrinsic motivation can be more effective, even though its application is less common. Other studies found that it can indeed positively affect compliance, and the results of correlating them with contributing factors of Cognitive Evaluation Theory (CET) should not be that surprising. It feels logical that the autonomy for local rulemaking and monitoring results in more compliance when you either made the rules yourself or explicitly agreed to them. It fits that competence influences rule compliance in participation because adherence is easier when you know how to do that. And also makes sense that relatedness results in less regulation violations in participation when you feel like you belong to the organization that made those rules. Although finding out why intrinsic motivation is not utilized more was not the focus of this study, understanding how it can be used was, which will be discussed next.

The deconstruction of non-compliance (chapter 2.4) proved instrumental in understanding successful utilization of intrinsic motivation for compliance, after correlation with solutions from other domains. The questionable results of cybersecurity awareness trainings demonstrate that solely externalizing[4] responsibility for compliance (chapter 2.3) towards employees is a failing strategy. Instead, reflecting on the implementation of policy (chapter 2.2), or indeed the style of governance (chapter 2.1) behind it, demonstrated to be more fruitful for increasing motivation (chapter 2.5) for compliance. For this reason, solutions are categorized under either governance or policy. However, during the course of this study other approaches were encountered which were less fitting for these categories, but nonetheless promising with regards to their positive effects on compliance. As such, communication and education were added as additional solution categories.

In the Governance (chapter 3.1) category, solutions that employ participation, self-regulation, and local rulemaking and monitoring were found. Participation (chapter 3.1.1) in cybersecurity is scarce [90, p. 61] and usually restricted to tokenism. It is understandable not all corporate levels of planning can be delegated to employees due to stakeholder and regulatory obligations. However, the participation levels for operational and tactical decisions and implementations could be raised. This may not only increase employee responsibility for organizational objectives as posed by Theory Y [48], but is also demonstrated to positively contribute to compliance. Both in nature preservation as well as the university experiment this result could be related to contributing aspects of CET, relatedness and competence, which provides a strong indication intrinsic motivation had a positive effect. I think the

[4] Some (meta)pun intended.

idea of decentralization in cybersecurity could be pushed further to effectuate this. The 'sharing of responsibility' usually stops at security officers or security specialists, still segregating 'regular employees' and 'security personnel'. By pushing this responsibility further out to operational personnel, such as product development, a higher degree of integration could be achieved which could logically result in more participation. Self-regulation (chapter 3.1.2) is in essence autonomy, the third contributing aspect of CET, and is most likely even less prevalent in cybersecurity given it's the highest level of participation. One of the main contributors to its successful application is a shared understanding between employees and employers [91, p. 1], in particular regarding goals. While Agency Theory [52] stipulates effective self-regulation is achieved by overriding behavior, a more effective approach may be closer alignment of corporate and employee ideology. In technology it was beliefs and ethics that inspired more adherence, and within law enforcement and defense it was values that minimized misconduct. I think this closer alignment could be achieved by shared creation of mission, vision, and strategy for cybersecurity, instead of being owned and written by a centralized security department. This could be implemented in a tiered approach, where this is indeed self-regulated at an operational level, deriving from a tactical and strategic level. Local rulemaking and monitoring (chapter 3.1.3) brings the addition of local monitoring. Full autonomous monitoring [58] has the same challenges as self-regulation, and care should be taken that trust between employees is not eroded due to peers observing their (relative) performance [92, p. 424]. However, it was found this approach might enhance intrinsic motivation, and autonomy (a contributing aspect to CET) in nature preservation demonstrated it increased compliance in combination with local rulemaking. I think local monitoring in cybersecurity could bring a lot of added value. It is the knowledge of local employees that could provide proper targeting and interpretation of monitoring, thus providing context for cybersecurity incidents. However, concepts like separation of duties and the tree lines of defense should still be adhered to because it is easy for employees' reputations to take a nosedive[5] when colleagues monitor each other.

In the Policy (chapter 3.2) category, solutions alleviating administrative burden and employing gamification were encountered. For Administrative burden (chapter 3.2.1) it is undeniable that corporations should introspect on their style of governance and the policy it produces, because this directly related [93, p. 1] to cybersecurity compliance costs [62] of employees as well as decreased compliance. In law enforcement compliance was increased when process friction was reduced, and in agriculture it was found compliance can be increased by granting more, which can be linked to intrinsic motivation. I think there could be a lot to gain by reduction and simplification of policy. The sheer amount of content employees are supposed to absorb, and the number of rules they have to abide by, is one of the bigger burdens imposed by cybersecurity policies. Additionally, a lot could be accomplished by standardization, which incorporates a cybersecurity baseline, and thus a level of security employees don't have to worry about anymore. While Gamification [65] (chapter 3.2.2) is abundant, and thus familiar, in cybersecurity [94, p. 586] it does deserve explicit mention within the context of this study since an increase in compliance with self- healthcare as well as in safety was observed. This no doubt explains its proliferation in cybersecurity. I think the forms of awareness trainings in cybersecurity could benefit from an overhaul, as currently a lot of employees consider it a nuisance that has to be dealt with periodically. Gamification could help with this although care should be taken it does not become 'just a

[5] Like in episode 1 of season 3 of the TV series Black Mirror.

game' that employees play for the fun of it. Instead, game mechanisms could be incorporated in other awareness activities to make those more engaging without resorting to an actual game.

In the Communication (chapter 3.3) category, a central role in solutions is framing, motivational interviewing, prosocial motivation, and autonomy-supportive behavior. (re)Framing (chapter 3.3.1) could be a relatively low-effort approach when it 'merely' requires rephrasing of communication frames [68] used in policy. Of course, any deriving implementation would have to be adjusted likewise, thus impacting operations as well. Additionally, care should be taken it does not take on the deceptive characteristics of spin doctoring, inevitably negating any increased compliance [95, pp. 8,43]. Framing, however, was demonstrated to be effective both in retail and during an experiment, thus showing potential for increasing compliance. I think framing is a good start for revising policies in cybersecurity but also needs to be accompanied by a new way of thinking or attitude change. For example, simply rephrasing 'the security department is responsible for cybersecurity' to 'we are all responsible for cybersecurity' changes something fundamental about responsibilities that needs to be addressed at a fundamental level. Otherwise, everybody will blame somebody when nobody did what anybody could have done[6]. Motivational interviewing [72] seems to be incompatible with a corporate environment. It relies heavily on one-on-one contact and challenges for groups-sessions have also been noted [96, p. 9]. Additionally, it requires specialized training for conversational techniques, and prior experience as a therapist or counselor seems implied. This is a shame given its close affiliation with intrinsic motivation, as a healthcare experiment demonstrated it changed attitudes towards compliance, and was further hypothesized to increase autonomy and being related to intrinsic motivation. I think it could be complex to apply to cybersecurity, especially given the skillset of the average security specialist or manager, and the requirements for practical application. Prosocial motivation [75] mostly seems to be related to employee attitude, which is in turn subjective to corporate culture [97, p. 361]. Serious consideration should be given to whether the benefits of this approach outweigh the risks, since achieving corporate culture change is notoriously difficult [98, p. 3]. When it does, an increase in compliance could be the results, as both a survey and experiments in healthcare demonstrated. I think this can be applied on a smaller scale in cybersecurity, such as a team level, where culture is probably easier to change and reliant on less individuals. However, I don't see many corporations taking such big steps, 'merely' to improve their cybersecurity posture. For Autonomy-Supportive Behavior (chapter 3.3.4), the potential and limitations in a corporate environment have in part been covered for self-regulation and local rulemaking and monitoring. Additionally, this approach relies on soft skills, which are not necessarily common in cybersecurity [99, p. 354]. Training 'customer facing' employees, such as security offers, could however be a good investment, as a survey in health and safety demonstrated it to contribute to compliance, and a survey in healthcare found it to support autonomy. Unsurprisingly, this could be related to intrinsic motivation. I think more autonomy would be beneficial for cybersecurity, especially at the employee level. However, cybersecurity, and indeed corporations in general, tend to have a hierarchical structure that is to some extend incompatible with this concept. Although there has been changes in recent years regarding agility and working supervisors, the general tendency still seems to lean towards command and control, which doesn't play well with autonomy.

Finally, in the Education (chapter 3.4) category solutions included bias correction and awareness training. Bias correction (chapter 3.4.1) illustrates human judgement is not flawless and requires some

[6] To paraphrase "Whose Job Is It, Anyway?", or "The Responsibility poem", by Charles Osgood.

adjustment from time to time. Although it has been demonstrated employees are prone to this flaw, the same can be read between the lines for employers. Employees can indeed exhibit non-compliant behavior, but employers seem to be biased about its contributing factors, and their own role in this. Questionnaires in technology and psychology demonstrated those biases can be corrected, which could in turn increase compliance. I think application in cybersecurity can and should be done but requires specialized personnel who can take an outside view and have had specialized training. Most likely, similar challenges as with culture changes will be encountered, as biases are probably deeply ingrained. Awareness training [85, p. 6] (chapter 3.4.2) seems to be a tried and tested approach to increase compliance, but why include it as a possible solution if its effectiveness is questionable? [100, p. 8] (perceived lack of) Knowledge is the main focus of such trainings, which we can assume to increase. However, resulting employee attitude and behavior tend not to be measured, which may well be the flaw. Regardless, the approach is demonstrated to be successful as compliance was increased both in a maritime industry survey as well as a university training. I think this approach could be improved in cybersecurity. However, it has been considered 'the silver bullet' for a lot of cybersecurity problems for too long and has failed to deliver on that promise. As such, it is probably best utilized less in favor of the other approaches. If one were so inclined, the most gain could be had from measuring results from trainings (over a longer period of time).

## 4.1 Limitations

Literature studies are inherently limited through the examination of encountered sources, and (omitted) sources not encountered. A different approach to the same type of study could yield additional results which may shed a different perspective on these findings. Additionally, other types of research could further enrich this study. For example, further examination of hypotheses from this thesis could be achieved either through surveys or field studies. As such, complete coverage of this topic has most likely not been attained. There is a plethora of research from other domains to be examined, correlated, and checked for counter arguments. However, by using multiple samples from several domains on the same topic a reasonable certainty about the encountered results could be ascertained. Additionally, the trans positioning of (hypothesized) solutions from other domains to cybersecurity from this thesis are inherently that, a hypothesis, be it based on my own practical work experience in the cybersecurity domain. As such, further research is required to determine their fit from both a scientific as well as a practical perspective.

## 4.2 Further research

This research touched upon some specific topics that could benefit from further research. It would be interesting to see how participation (chapter 3.1.1), and levels of collaboration, could lead to increased motivation (chapter 2.5) through internalization. This topic is closely tied into decentralization, and a new governance (chapter 2.1) approach. These topics have potential to increase compliance (chapter 2.3) by shifting the focal point of responsibility for cybersecurity, but require more concrete examination to explore their potential. Another interesting field of research is that of communication (chapter 3.3), specifically the motivational factors as well as framing (chapter 3.3.1). These have the potential of closing the rift between 'security' and 'the business' which, although growing smaller, still exists within the industry.

## 4.3 Conclusion

This study set out to answer how other domains are using motivation (chapter 2.5) to increase compliance (chapter 2.3), and whether these approaches could be applied in cybersecurity. The results show that the common approach to attain compliance in cybersecurity employs extrinsic motivation, usually through punitive actions based on General Deterrence Theory (GDT). However, by studying approaches from other domains it was found that intrinsic motivation could be an alternative approach to stimulate compliance, by fostering autonomy, competence, and relatedness from Cognitive Evaluation Theory (CET). Over half of the alternative approaches from other domains that increased compliance could be related to one or more of these contributing factors of CET, either directly or indirectly. This indicates CET is a viable foundation for alternative solutions in the cybersecurity domain. Further research is required for practical application, for which several possible approaches have been hypothesized in this study.

# 5 Bibliography

[1] Thales, "From Ukraine to the whole of Europe:cyber conflict reaches a turning point," 29 03 2023. [Online]. Available: https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point. [Accessed 06 07 2023].

[2] P. Schläpfer, "Magniber Ransomware Targets Users with Fake Software Updates," Hewlett-Packard, 13 10 2022. [Online]. Available: https://threatresearch.ext.hp.com/magniber-ransomware-switches-to-javascript-targeting-home-users-with-fake-software-updates/. [Accessed 25 04 2023].

[3] E. Kovacs, "Nation-State Hacker Attacks on Critical Infrastructure Soar: Microsoft," SecurityWeek, 07 11 2022. [Online]. Available: https://www.securityweek.com/nation-state-hacker-attacks-critical-infrastructure-soar-microsoft/. [Accessed 25 04 2023].

[4] A. Greenberg, "Hacker Lexicon: What Is a Supply Chain Attack?," Wired, 31 05 2021. [Online]. Available: https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/. [Accessed 25 04 2023].

[5] D. Thomas, "Your Facebook posts could help hackers guess your password," Bluegrass, 31 01 2022. [Online]. Available: https://bluegrass-group.com/your-facebook-posts-could-help-hackers-guess-your-password/. [Accessed 25 04 2023].

[6] I. Ivanova, "Equifax ex-CEO: Hacked data wasn't encrypted," CBS News, 03 10 2017. [Online]. Available: https://www.cbsnews.com/news/equifax-ex-ceo-hacked-data-wasnt-encrypted/. [Accessed 05 04 2023].

[7] Y. So-Yeon, "Police raid office of game developer accused of data theft," Korea JoongAng Daily, 8 03 2023. [Online]. Available: https://koreajoongangdaily.joins.com/2023/03/08/business/tech/Korea-Game-Nexon/20230308173216734.html. [Accessed 25 04 2023].

[8] P. Puhakainen and M. Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly,* vol. 34, no. 4, pp. 757-778, 2010.

[9] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems,* vol. 18, no. 2, pp. 101-105, 2009.

[10] C. Ansel and J. Torfing, Handbook on Theories of Governance, Cheltenham: Edward Elgar Publishing Limited, 2022.

[11] B. G. Peters and J. Pierre, Comparative Governance - Rediscovering the Functional Dimension of Governing, Cambridge: Cambridge University Press, 2016.

[12] P. Katsamunska, "The Concept of Governance and Public Governance Theories," *Economic Alternatives,* no. 2, pp. 133-141, 2016.

[13] M. Maesschalck, Reflexive Governance for Research and Innovative Knowledge, London: Wiley-ISTE, 2017.

[14] J. Pierre and B. G. Peters, Governance, Politics and the State, London: RED GLOBE PRESS, 2020.

[15] B. Jessop, "Governance and meta-governance: On reflexivity, requisite variety and requisite irony," in *Governance as social and political communication*, Manchester University Press, 2003, pp. 101-116.

[16] T. Tropina and C. Callanan, Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, Cham: Springer, 2015.

[17] J. E. Anderson, Public Policymaking: An Introduction, Boston: Houghton Mifflin Company, 2003.

[18] H. Leavitt, "Applied organization change in industry: structural, technical, and human approaches," 1964. [Online]. Available: https://archive.org/details/newperspectivesi0000coop/page/54/mode/2up. [Accessed 05 01 2023].

[19] B. Schneier, ""People, Process, and Technology"," 30 01 2013. [Online]. Available: https://www.schneier.com/blog/archives/2013/01/people_process.html. [Accessed 05 01 2023].

[20] National Institute of Standards and Technology, "Uses and Benefits of the Framework," 8 12 2021. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework. [Accessed 02 02 2023].

[21] International Organization for Standardization, "ISO/IEC 27000," 2018. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip. [Accessed 02 02 2023].

[22] M. L. Mueller, Networks and States: The Global Politics of Internet Governance, Cambridge: The MIT Press, 2010.

[23] S. A. Adams, M. Brokx, L. D. Corte, M. Galič, K. Kala, B.-J. Koops, R. Leenes, M. Schellekens, K. e. Silva and I. Škorvánek, "The Governance of Cybersecurity," 11 2015. [Online]. Available: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/91923.PDF. [Accessed 04 04 2023].

[24] D. J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," 15 05 2019. [Online]. Available: https://web.archive.org/web/20190515210006/https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/. [Accessed 04 04 2023].

[25] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," 01 2020. [Online]. Available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468. [Accessed 04 04 2023].

[26] Ministerie van Economische Zaken en Klimaat, "Regeling veiligheid en integriteit telecommunicatie," 01 10 2021. [Online]. Available: https://zoek.officielebekendmakingen.nl/stcrt-2021-42618.html. [Accessed 04 04 2023].

[27] C. Peukert, S. Bechtold, T. Kretschmer and M. Batikas, "Regulatory export and spillovers: How GDPR affects global markets for data," Centre for Economic Policy Research, 30 09 2020. [Online]. Available: https://cepr.org/voxeu/columns/regulatory-export-and-spillovers-how-gdpr-affects-global-markets-data. [Accessed 05 04 2023].

[28] Cambridge University Press, "Compliance | English meaning," Cambridge Dictionary, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/compliance. [Accessed 05 01 2023].

[29] T. Hobbes, Leviathan, 1660.

[30] W. C. Bailey, J. D. Martin and L. N. Gray, "Crime and Deterrence: A Correlation Analysis," *Journal of Research in Crime and Delinquency,* vol. 11, no. 2, pp. 124-143, 1974.

[31] R. Paternoster, "HOW MUCH DO WE REALLY KNOW ABOUT CRIMINAL DETERRENCE?," *The journal of criminal law & criminology,* vol. 100, no. 3, pp. 765-824, 2010.

[32] International Organization for Standardization, "ISO/IEC 27001," 2013. [Online]. Available: http://www.itref.ir/uploads/editor/42890b.pdf. [Accessed 10 01 2023].

[33] Information Systems Audit and Control Association, COBIT 5 for Information Security, 2012.

[34] E. Cole, "Insider Threats and the Need for Fast and Directed Response," 04 2019. [Online]. Available: https://informationsecurity.report/Resources/Whitepapers/4b2d1b48-5c20-48bb-b08b-eb7ff295fdff_insider-threats-need-for-fast-directed-response-pdf-3-w-2031.pdf. [Accessed 03 01 2023].

[35] Verizon, "2022 Data Breach Investigations Report," 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2022-data-breach-investigations-report-dbir.pdf. [Accessed 03 01 2023].

[36] E. Kolkowska, F. Karlsson and K. Hedström, "Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method," *Journal of Strategic Information Systems,* vol. 26, no. 1, pp. 39-57, 2017.

[37] C. Posey and M. Shoss, "Why Employees Violate Cybersecurity Policies," Harvard Business Review, 20 01 2022. [Online]. Available: https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies. [Accessed 10 01 2023].

[38] Cambridge University Press, "Motivation | English meaning," Cambridge Dictionary, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/motivation. [Accessed 16 01 2023].

[39] E. L. Deci and R. M. Ryan, Intrinsic motivation and self-determination in human behavior, New York: Springer Science+Business Media, 1985.

[40] D. Jovanovic and M. Matejevic, "Relationship between Rewards and Intrinsic Motivation for Learning – Researches Review," *Procedia - Social and Behavioral Sciences,* vol. 149, pp. 456-460, 2014.

[41] J. P. D'Arcy, "Security countermeasures and their impact on information systems misuse: A deterrence perspective," 2005. [Online]. Available: https://www.proquest.com/docview/305440773?pq-origsite=gscholar&fromopenview=true. [Accessed 17 01 2023].

[42] K. Irwin, L. Mulder and B. Simpson, "The Detrimental Effects of Sanctions on Intragroup Trust: Comparing Punishments and Rewards," *Social Psychology Quarterly,* vol. 77, no. 3, pp. 253-272, 2014.

[43] J. L. Howard, J. Bureau, F. Guay, J. X. Y. Chong and R. M. Ryan, "Student Motivation and Associated Outcomes: A Meta-Analysis From Self-Determination Theory," *Perspectives on Psychological Science,* vol. 16, no. 6, pp. 1300-1323, 2021.

[44] E. L. Deci, R. Koestner and R. M. Ryan, "Extrinsic Rewards and Intrinsic Motivation in Education: Reconsidered Once Again," *Review of Educational Research,* vol. 71, no. 1, pp. 1-27, 2001.

[45] K. Osei-Frimpong, "Patient participatory behaviours in healthcare service delivery: Self-determination theory (SDT) perspective," *Journal of Service Theory and Practice,* vol. 27, no. 2, pp. 453-474, 2017.

[46] J.-Y. S. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Information & Management,* vol. 48, pp. 296-302, 2011.

[47] V. C. Lee, "Examining the Relationship between Autonomy, Competence, and Relatedness and Security Policy Compliant Behavior," 10 2015. [Online]. Available: https://www.proquest.com/docview/1746623306. [Accessed 20 01 2023].

[48] D. McGregor, The Human Side of Enterprise, New York: McGRAW-HILL BOOK COMPANY, 1960.

[49] S. R. Arnstein, "A Ladder Of Citizen Participation," *Journal of the American Institute of Planners,* vol. 35, no. 4, pp. 216-224, R..

[50] C. Viteri and C. Chávez, "Legitimacy, local participation, and compliance in the Galápagos Marine Reserve," *Ocean & Coastal Management,* vol. 50, no. 3-4, pp. 253-274, 2007.

[51] D. A. DeCaro, M. A. Janssen and A. Lee, "Synergistic effects of voting and enforcement on internalized motivation to cooperate in a resource dilemma," *Judgment and Decision Making,* vol. 10, no. 6, p. 511–537, 2015.

[52] R. F. Baumeister, B. J. Schmeichel and K. D. Vohs, "Self-regulation and the executive function: The self as controlling agent.," in *Social psychology: Handbook of basic principles*, New York, The Guilford Press, 2007, p. 516–539.

[53] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," *Journal of Financial Economics,* vol. 3, no. 4, pp. 305-360, 1976.

[54] H. Li, R. Sarathy, J. Zhang and X. Luo, "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance," *Information Systems Journal,* vol. 24, no. 6, pp. 479-502, 2014.

[55] T. R. Tyler, P. E. Callahan and J. Frost, "Armed, and Dangerous (?): Motivating Rule Adherence among Agents of Social Control," *Law & Society Review,* vol. 41, no. 2, pp. 457-492, 2007.

[56] L. J. Rusch, "Separation of Powers Analysis as a Method for Determining the Validity of Federal District Courts' Exercise of Local Rulemaking Power: Application to Local Rules Mandating Alternative Dispute Resolution," *Connecticut Law Review,* vol. 23, no. 3, pp. 483-565, 1991.

[57] D. Osborne and T. Gaebler, Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector, Reading: Addison-Wesley Publishing Company, 1993.

[58] F. Danielsen, N. D. Burgess, A. Balmford, P. F. Donald, M. Funder, J. P. G. Jones, P. Alviola, D. S. Balete, T. Blomley, J. Brashares, B. Child, M. Enghoff, J. Fjeldså, S. Holt, H. Hübertz, A. E. Jensen, P. M. Jensen, J. Massao, M. M. Mendoza, Y. Ngaga, M. K. Poulsen, R. Rueda, M. Sam, T. Skielboe, G. Stuart-hill, E. Topp-jørgensen and D. Yonten, "Local Participation in Natural Resource Monitoring: a Characterization of Approaches," *Conservation Biology,* vol. 23, no. 1, p. 31–42, 2008.

[59] G. Epstein, "Local rulemaking, enforcement and compliance in state-owned forest commons," *Ecological Economics,* vol. 131, pp. 312-321, 2017.

[60] T. Hayes and L. Persha, "Nesting local forestry initiatives: Revisiting community forest management in a REDD+ world," *Forest Policy and Economics,* vol. 12, no. 8, pp. 545-553, 2010.

[61] E. Schlager and E. Ostrom, "Property-Rights Regimes and Natural Resources: A Conceptual Analysis," *Land Economics,* vol. 68, no. 3, pp. 249-262, 1992.

[62] D. Moynihan, P. Herd and H. Harvey, "Administrative Burden: Learning, Psychological, and Compliance Costs in Citizen-State Interactions," *Journal of Public Administration Research and Theory,* vol. 25, no. 1, pp. 43-69, 2015.

[63] E. Linos and N. Riesch, "Thick Red Tape and the Thin Blue Line: A Field Study on Reducing Administrative Burden in Police Recruitment," *Public Administration Review,* vol. 80, no. 1, pp. 92-103, 2020.

[64] C. Ritzel, G. Mack, M. Portmann, K. Heitkämper and N. El Benni, "Empirical evidence on factors influencing farmers' administrative burden: A structural equation modeling approach," *PLoS ONE,* vol. 15, no. 10, pp. 1-16, 2020.

[65] C. A. Coonradt, The game of work - How to enjoy work as much as play, Salt Lake City: Shadow Mountain, 1984.

[66] J. A. Cafazzo, M. Casselman, N. Hamming, D. K. Katzman and M. R. Palmert, "Design of an mHealth App for the Self-management of Adolescent Type 1 Diabetes: A Pilot Study," *Journal of Medical Internet Research,* vol. 14, no. 3, pp. 1-13, 2012.

[67] R. M. C. Leite, D. B. Costa, H. M. M. Neto and F. A. Durão, "Gamification technique for supporting transparency on construction sites: a case study," *Engineering Construction & Architectural Management,* vol. 23, no. 6, pp. 801-822, 2016.

[68] J. N. Druckman, "The Implications of Framing Effects for Citizen Competence," *Political Behavior,* vol. 23, no. 3, p. 225–256, 2001.

[69] D. A. Scheufele, "Framing as a Theory of Media Effects," *Journal of Communication,* vol. 49, no. 1, p. 103–122, 1999.

[70] Y. Feldman and O. Perez, "Motivating Environmental Action in a Pluralistic Regulatory Environment: An Experimental Study of Framing, Crowding Out, and Institutional Effects in the Context of Recycling Policies," *Law & Society Review,* vol. 46, no. 2, pp. 405-442, 2012.

[71] E. Fehr and S. Gächter, "Do Incentive Contracts Undermine Voluntary Cooperation?," 29 10 2002. [Online]. Available: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID313028_code020520670.pdf?abstractid=313028&mirid=1. [Accessed 02 03 2023].

[72] W. R. Miller and S. Rollnick, Motivational Interviewing: Helping People Change, New York: The Guilford Press, 2013.

[73] C. E. Golin, J. Earp, H.-C. Tien, P. Stewart, C. Porter and L. Howie, "A 2-Arm, Randomized, Controlled Trial of a Motivational Interviewing-Based Intervention to Improve Adherence to Antiretroviral Therapy (ART) Among Patients Failing or Initiating ART," *JAIDS Journal of Acquired Immune Deficiency Syndromes,* vol. 42, no. 1, p. 42–51, 2006.

[74] M. Vansteenkiste and K. M. Sheldon, "There's nothing more practical than a good theory: Integrating motivational interviewing and self-determination theory," *British Journal of Clinical Psychology,* vol. 45, no. 1, pp. 63-82, 2006.

[75] M. L. Hoffman, "Development of Prosocial Motivation: Empathy and Guilt," in *The Development of Prosocial Behavior*, New York, ACADEMIC PRESS, 1982, pp. 281-313.

[76] C. D. Batson, "Prosocial Motivation: Is it ever Truly Altruistic?," *Advances in Experimental Social Psychology,* vol. 20, pp. 65-122, 1987.

[77] Y. Chen, W. Xia and K. Cousins, "Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence," *Computers & Security,* vol. 113, pp. 1-20, 2022.

[78] A. M. Grant and D. A. Hofmann, "It's not all about me: motivating hand hygiene among health care professionals by focusing on patients," *Psychological Science,* vol. 22, no. 11, pp. 1494-1499, 2011.

[79] I. Burstyn, L. Jonasi and T. C. Wild, "Obtaining compliance with occupational health and safety regulations: a multilevel study using self-determination theory," *International Journal of Environmental Health Research,* vol. 20, no. 4, pp. 271-287, 2010.

[80] G. C. Williams, G. C. Rodin, R. M. Ryan, W. S. Grolnick and E. L. Deci, "Autonomous Regulation and Long-Term Medication Adherence in Adult Outpatients," *Health Psychology,* vol. 17, no. 3, pp. 269-276, 1998.

[81] Psychological scales, "Health Care Climate Questionnaire HCCQ," [Online]. Available: https://scales.arabpsychology.com/s/the-health-care-climate-questionnaire-hccq/. [Accessed 17 04 2023].

[82] A. Tversky and D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty.," *Science,* vol. 185, no. 4157, pp. 1124-1131, 1974.

[83] R. D. Cooter, M. Feldman and Y. Feldman, "The Misperception of Norms: The Psychology of Bias and the Economics of Equilibrium," *Review of Law & Economics,* vol. 4, no. 3, pp. 889-911, 2008.

[84] D. M. Messick, S. Bloom, J. P. Boldizar and C. D. Samuelson, "Why we are fairer than others," *Journal of Experimental Social Psychology,* vol. 21, no. 5, pp. 480-500, 1985.

[85] Information Security Forum, "Effective security awareness – workshop report," 02 04 2002. [Online]. Available: https://docplayer.net/storage/21/1261050/1680991732/X9ZDzQYEpZ5Rvy8zYk8TDQ/1261050.pdf. [Accessed 08 04 2023].

[86] S. Briggs, The home front : war years in Britain, 1939-1945, London: American Heritage Publishing Co. Inc., 1975.

[87] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & Security,* vol. 25, no. 4, pp. 289-296, 2006.

[88] E. D'agostini and S. Jo, "Maritime Security Training: Evaluation of the Impact on Seafarers' Security Awareness and Security Performance," *Journal of the Korean Society of Marine Environment & Safety,* vol. 25, no. 2, pp. 201-211, 2019.

[89] M. Sas, G. Reniers, K. Ponnet and W. Hardyns, "The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour," *employees' knowledge, attitude and self-reported behaviour,* vol. 144, pp. 895-900, 2021.

[90] W. A. Solomon, "Information Security Standards And Policies Compliance By Nigerian Banks," 2019. [Online]. Available: https://core.ac.uk/download/pdf/517438051.pdf. [Accessed 22 04 2023].

[91] R. F. Baumeister and T. F. Heatherton, "Self-Regulation Failure: An Overview," *Psychological Inquiry,* vol. 7, no. 1, pp. 1-15, 1996.

[92] G. Sewell, "The Discipline of Teams: The Control of Team-Based Industrial Work through Electronic and Peer Surveillance," *Administrative Science Quarterly,* vol. 43, no. 2, pp. 397-428, 1998.

[93] C. Herley, "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," 04 2009. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/SoLongAndNoThanks.pdf. [Accessed 23 04 2023].

[94] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane and D. Weintrop, "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games," *Simulation & Gaming,* vol. 51, no. 5, pp. 586-611, 2020.

[95] B. Stockman, "The influence of spin doctors on political communications," 2007. [Online]. Available: http://www.agnesbruneel.be/bentxi/project%20spin_final.pdf. [Accessed 23 04 2023].

[96] C. C. Wagner and K. S. Ingersoll, "Introduction," in *Motivational Interviewing in Groups*, New York, Guilford Press, 2012, pp. 3-12.

[97] J. Malcolmson, "What is security culture? Does it differ in content from general organisational culture?," 13 11 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5335511. [Accessed 23 04 2023].

[98] Institute for Corporate Productivity, "Culture Renovation® Executive Brief," 2019. [Online]. Available: https://go.i4cp.com/culturerenovationbrief. [Accessed 23 04 2023].

[99] J. L. Hall and A. Rao, "Non-Technical skills needed by cyber security graduates," in *2020 IEEE Global Engineering Education Conference (EDUCON)*, Porto, 2020.

[100] T. Caldwell, "Making security awareness training work," *Computer Fraud & Security,* vol. 2016, no. 6, pp. 8-14, 2016.