Adoption of cybersecurity innovations – a systematic literature review

Arnstein Vestad[1][0000-0002-7013-3322] and Bian Yang[1][0000-0001-6189-1976]

[1] NTNU, Norwegian University of Science and Technology, Norway

Abstract. Adoption of new cybersecurity capabilities in an organization can be seen as examples of adoption of technological innovations. While regulators use rules, standards and codes of practice to influence the state of cybersecurity in regulated organizations – other factors, such as technological complexity, organizational size, management support have been shown to influence technological adoption. Limited empirical research exists on factors influencing cybersecurity implementation in organizations. Existing models have focused on productivity or leisure applications - adoption of security innovations is fundamentally different because their adoption is founded on the intention to prevent incidents in the future with limited direct positive gain. A systematic literature review on existing research on adoption of security innovations is presented and suggestions for further research in more quantitative measures for the drivers of organizational cybersecurity technology adoption is suggested.

Keywords: cybersecurity, technology adoption, innovation

1 Introduction

Cybersecurity is an arms race between attackers and defenders continually driven by innovations in both attacker and defender techniques, tools and tactics. For each new attack technique organizations, and the security industry, is driven to innovate, develop, market and adopt new countermeasures in a continually changing risk landscape. The continually increasing interconnectedness through IoT, industry 4.0, smart cities and cyber physical systems change attack and defense possibilities and capabilities giving little pause for defenders.

For organizations seeking to protect their information assets, IT systems and services, there is no lack of advice, frameworks, standards, products and services. As in all marketplaces, some innovations succeed while others fall by the wayside. But for organizations choosing to adopt innovative cybersecurity technologies the adoption inherently implies risk - the risk of adopting technologies that doesn't live up to its purported potential or that loses support from its vendors as well as the potential of wasted time and resources on building product specific skill and competencies in the internal organization.

The rate of innovation in the cybersecurity market is high - by innovation we understand implementing something new or significantly improving upon existing products,

services, processes – this will be time dependent, while firewalls were once an innovation, implementing SaaS and cloud based security technologies may now be classified as innovations. This rate of innovation is posing several challenges for organizations wanting to adopt them – both in identifying relevant innovations, understanding how the innovations fit existing technologies in the organization, integrating them as well as educating the cybersecurity workforce to be able to operate and take full advantage of the innovations. Cybersecurity investments also primarily show their value in a reactive way by preventing incidents – and as cybersecurity attacks and incidents are often complex and can take many paths, it can be hard to estimate the precise value and contribution of each investment.

Several theoretical frameworks exist to explain how and why organizations adopt technologies and innovations – from the initial theories of Diffusion of Innovation[1] explaining various characteristics of innovations (complexity, trialability, observability etc.) and the social mechanisms through which innovations spread, to variants of the Technology Acceptance Model[2] where perceived usefulness and perceived ease of use affects attitude and intention to use a new technology. Traditional technology acceptance models have been critiqued for not being sufficient when the technology adopted is a security technology, and the value of the product is not related to its usefulness directly, but to its ability to prevent future harm – theoretical models with roots in preventive medicine has therefore also been used, such as Protection Motivation Theory[3] and Health Belief models, that account for how perceptions of vulnerability and the effectiveness of preventive measures affect attitudes towards preventive measures.

Understanding the drivers of cybersecurity adoption has the potential to increase societal security by allowing policy makers, regulators and industry stakeholders to develop policies and engage in activities that promote organizational uptake of cybersecurity technology. While previous surveys have reviewed organizational security on the policy level [4], and reviewed literature on specific types of adoption theories, such as Deterrence theory [5], the intention of the current paper is to give a survey and a broader overview of the existing main theories used to explain the drivers behind cybersecurity technology adoption, to describe their main concepts and how they have been adapted by researchers to fit cybersecurity specific issues, and give suggestions for further development of the understanding of organizational cybersecurity adoption.

The contributions of this research is mainly to:

- Contribute to a better understanding of the factors affecting cybersecurity innovation implementation in organizations
- Allow stakeholders and practitioners to focus on the adoption measures that most significantly affect adoption and implementation of innovative cybersecurity capabilities
- Serve as a foundation to develop improved approaches to measuring and improving cybersecurity innovation adoption in organizations

This paper first presents the theoretical background of the major technology adoption models, firstly general technology adoption theories followed by adoption theories rooted in preventive health that take into account risk, vulnerability etc. We then present

the literature review methodology before presenting our findings, including the research based on the various models, as well as what extensions researchers have suggested to adapt their research models towards cybersecurity.

2 Theoretical background

Rogers Diffusion of Innovation[1] (DoI) framework has been the leading theoretical framework for understanding the diffusion and adoption of innovations from an individual and organizational perspective. Rogers describes a five phased adoption process for individual adoption of innovations consisting of the phases knowledge, persuasion, decision, implementation and confirmation/continuation. Likewise, on an organizational level, he described a process consisting of agenda setting, matching, redefining/restructuring, clarifying and routinizing, where the organization moves from initial problem awareness and identification of the need for innovation, to the innovation becoming a normal part of the organizations work processes. To explain the rate of adoption, Rogers described five primary characteristics of an innovation that contribute to the adoption – the innovation´s relative advantage, compatibility, complexity, trialability and observability.

Innovation adoption have been studied from both a process and a factors perspective[2] – the process perspective studies the behavior and progression over time of the organization in its adoption of innovations, while the factors perspective studies the attributes that influence, facilitate or inhibit the adoption process. In the organizational perspective the adoption of technology in an organization is often divided in two main phases – firstly the organizational decision process where typically the organizations management decides on introducing a new technology, and the later phase where the technology needs to be implemented and assimilated into the organization, affecting routines, work processes and organizational culture.

2.1 Technology acceptance models

While DoI is a generic model for the diffusion of ideas and innovations of all kinds, the Technology Acceptance Model [3] (TAM) has been one of the leading frameworks for reasoning about technological acceptance and adoption[4]. The framework builds on Aizen and Fishbeins Theory of Reasoned Action (TRA) [5] as a theoretical basis. While TRA is a very generic model, useful for explaining general behavior, the TAM was designed to apply only to computer usage behavior. TRA is based on the concepts that a person's behavior is determined by the persons *behavioral intention*, which again is determined by *attitude* towards the behavior and *subjective norm* (the perception of what others around the person think about the behavior, as well as the persons motivation to comply with this social pressure.

In the Theory of planned behavior (TBP)[6], Aizen added the concept of *Perceived behavioral control*, to improve the predictive power of TRA, a concept grounded in psychological theories of self-efficacy – the individuals perceptions of their own

abilities to successfully implement the behavior. This perception interacts with *attitude* and *subjective norm*, and collectively these concepts affect behavioral intention.

TRA and TPB leaves open exactly what contributes to the beliefs for a specific behavior. To address this, TAM seeks to develop a model directly related to computer use and technology acceptance. TAM leaves out TRA's subjective norm, arguing that this is less understood and difficult to disentangle from the subjective norms indirect effects via attitude. In TAM, the attitude towards technology use is determined by the perception of *Ease of use*, and the perception of *Usefulness.* In the original TAM, usefulness is described as "the subjective probability that using a particular application system will increase his or her job performance within an organizational context".

Venkatesh and Davis extended the TAM to better explain the concept of *Perceived usefulness* in TAM2[4], also reintroducing the *subjective norm* from TRA affecting both *perceived usefulness* and *intention to use*. Subjective norm was however found to be dependent on the degree of *voluntariness* - when use is mandatory, as is often the case in an organizational setting, *social norm* has little effect on intention to use (but may still influence *perceived usefulness* – leaving room for improving adoption through social persuasion). *Subjective norm* also influences *image*, that is the individuals perception of how the innovation affects their social status among peers – and *image* influences *perceived usefulness*. The users direct *experience* with the innovation over time, also reduces the effect of *subjective norm*. *Job relevance*, *output quality* and *result demonstrability*, the more direct experience that the technology contributes to the job performance of the user. The users *experience* also affect the *social norm* – as a user is more acquainted with the system he or she is more likely to rely on personal evaluation to determine usefulness.

TAM2 was further developed into TAM3 by Venkatesh and Bala[7] seeking to better explain *perceived ease of use* from the original TAM. Here determinants of perceived ease of use are *Computer self-efficacy*, *perception of external control, computer anxiety, computer playfulness, perceived enjoyment* and *objective usability*.

In the Unified theory of acceptance and use of technology (UTAUT)[8], Venkatesh et al. reviewed eight theories of user acceptance and developed a unified model. The original concepts of *Behavioral intention* leading to *Use behavior* are consistent with TRA, but four new concepts that drive behavioral intention are *Performance expectancy* (largely similar to *perceived usefulness* from TAM), *Social influence* (similar to *subjective norm* from TRA and TAM), *Effort expectancy* (similar to perceived ease of use from TAM), and *Facilitating conditions* (defined as "the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system") – this concept influencing *actual use behavior*, that is, when the necessary conditions for forming a behavioral intention is present, the actual use is also modified by the facilitating conditions in the organization. The concepts of *gender, age, experience* and *degree of voluntariness* also serve as moderators of the interactions in the model. While the original UTAUT was originally defined in an organizational context, the model was further developed into UTAUT2[9], to better account for behavior in a consumer context, removing the moderating effect of *voluntariness* and adding the new concepts of *hedonic motivation, price value* and *habit*.

Another framework widely used to explain technology adoption in organizations is the Technology – organization – environment (TOE) framework[10]. The framework seeks to explain innovation adoption through three contextual influences that affect the organization. Firstly the technology itself, secondly intraorganizational factors such as internal communication, management communication, organizational structure and size and slack capacity in the organization and thirdly environmental factors such as the structure of the industry, availability of service providers to aid in implementation as well as regulatory pressures that inhibit or promote innovation.

The TOE framework is a very generic framework, and researchers have used the framework to explain technological adoption in many different settings and adapted the framework to account for the technologies being researched[11], and this is considered both a strength and a weakness of the model – since the model is rarely similar across research areas, direct comparisons can be difficult, but the flexibility and continued use have also shown its power to serve as a theoretical framework for understanding organizational adoption processes.

2.2 Preventive models

The application of general technology adoption frameworks has been critiqued for not properly accounting for cybersecurity technologies, in particular because their initial focus on adoption of productivity technologies in organizations, or in later iterations, more consumer oriented, hedonistic applications[9]. For example, [12] argue that TAM models do not include the concept of threat. Also, [13] found limited support for the concepts of *ease of use* and *attitude*, and between *self-efficacy* and perceived behavioral control – arguably because the use of protection technologies is driven more by the threat of unwanted incidents than by direct benefits of the technology.

There are several factors that contribute to making cybersecurity innovations different from “normal” innovations:

- There is little immediate, visible gain from security technologies so the value of security may be seen as more abstract, especially compared to the directly observable costs of implanting the technology[14].
- Adoption of security technologies are often seen as a way to manage risk – and can be seen from an economic perspective to be a calculation comparing the cost of the security technology against an assumed cost of a security incident, and this cost being an expected value of the likelihood of the incident (as driven by threats and vulnerabilities) and the impact (driven by the valuation of the impacted assets)
- Cybersecurity is adversarial and the threats that needs to be defended against are continually changing, new vulnerabilities and attack tactics are continuously developed – adoption of security technologies have to be a continuous process of evaluating and prioritizing investments.

Adoption of cybersecurity innovations may be seen as examples of adoption of preventive behavior, and several theories with roots in preventive health theory have been used to explain the adoption, on individual or organizational level, of

cybersecurity innovations. These theories are based on a concept of security behavior being similar to adopting positive health behaviors, such as taking up exercise and quitting smoking, that like security technology is prescribed to prevent unwanted incidents (a disease, bad health) that constitute threats, and imply a perception of the threat, the patients perception of their own susceptibility to the threat as well as their perception of how they might avoid the threat.

The Health belief model (HBM) was initially developed in the early 1950s to explain behavior surrounding the adoption of disease prevention measures in the population or participating in screening tests for diseases. The model posits that in order to take action to prevent a disease, the individual firstly must have a perception of their *susceptibility* to the disease as well as the *severity*. The individual would also have a perception of the *benefits* of taking action as well as take into account any *barriers* to taking action. In addition, *cues to action*, internal or external, such as symptoms or public health warnings, facilitate the action.

Protection motivation theory[15] (PMT) is a similarly grounded theory that posits a protection motivation calculus based on a *threat appraisal* that takes into account the *severity* and the *vulnerability*, in addition to the *rewards*, or benefit of taking action, as well as a *coping appraisal* that takes into account the perception of *response efficacy*, that is how likely the action is considered to be successful, as well as *self-efficacy*, an evaluation of the individuals ability to perform the action.

The Fear Appeals Model [12] (FAM) is an extension of protection motivation theory that incorporates TAM concepts of *social influence* and *behavioral intent* (but not *performance expectancy* that was found insignificant in pilot testing of the model). The model is intended to explain the intention of performing protective behaviors (in the study, implementing protection against spyware) recommended through “fear inducing persuasive communication”. One central finding was that people react differently to fear communication, some may be inspired to take protective action, while others reject the fear appeal and take action to reduce their fear instead.

The Technology Threat Avoidance Theory build on the health belief model and risk analysis models to posit three main processes of *threat appraisal, coping appraisal* and *coping*. The threat appraisal is an evaluation of the perceived threat taking into account the perceived *susceptibility* and perceived *severity*. The coping appraisal takes into account the perceived *effectiveness*, perceived *costs* and *self-efficacy* giving rise to a perceived *avoidability*, that is, how likely is the adoption of the preventive measure to succeed in avoiding the unwanted outcome. The threat appraisal and the coping appraisal drives the *avoidance motivation* and *avoidance behavior* in a problem focused *coping* process – however, if the perceived *avoidability* is low, the individual might resort to emotion focused coping behavior (for example - hoping to avoid or choosing to accept the unavoidable).

3 Literature review on the diffusion of cybersecurity innovations

In order to investigate how the cybersecurity literature has approached the question of motivation to adopt cybersecurity measures a literature review was performed – two

major databases, Scopus.com and the AIS Digital Library was searched, as these together give good coverage in both the IS and CS domains.

Title, abstract and keywords were searched for the terms :

```
("cyber security" OR "cybersecurity" OR "information security" ) AND ( "technology acceptance" OR "technology adoption" )
```

Articles not describing adoption processes, and articles describing the effect of security/trust evaluations on the adoption of other technologies were excluded from the survey. As our focus is on the drivers of adoption, papers describing the effect of adoption, for example on corporate profit have been excluded.

The search resulted in 158 papers from Scopus.com and 824 papers from the AIS digital library (in addition to two papers found by snowballing method from the reviewed papers). After screening of abstracts 904 papers were excluded according to the inclusion criteria and 9 papers were not available for access. 69 papers were assessed for eligibility by full text reading. After reading an additional 28 papers were excluded, resulting in a total of 41 papers included in this review. A high number of papers were excluded in the initial abstract screening process, this due to the quite generic search terms. A PRISMA diagram of the review process is presented in figure 1.

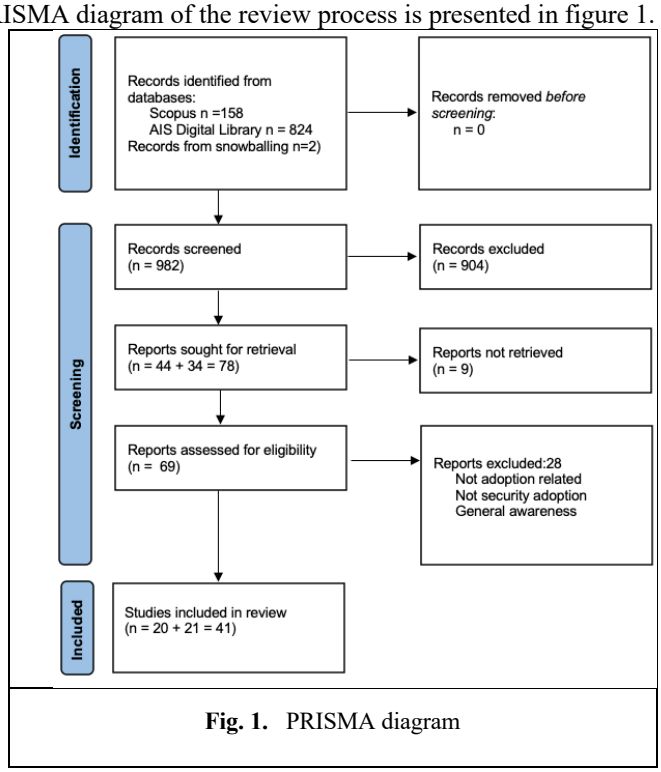

Fig. 1. PRISMA diagram

A summary of the reviewed papers as to what main model they are based on ("Main model"), the central concepts of the main models ("Central Concepts") and extensions

that researchers have added ("Suggested extensions") to the models are given in table 1. Several studies used more than one framework and are mentioned under more than one "main model". Several also referenced some of the precursor frameworks to the main framework(s) of the research, these are not mentioned in the table.

Table 1. Summary of identified papers, the central concepts used and the authors suggested extensions to the main models

Main model	Central concepts	References	Suggested extensions
Health Belief Model[16]	Perceived susceptibility, Perceived seriousness, Perceived benefits, Barriers, Cues to action	[17], [18]	Normalization Process theory to explain continued adoption: Tool cohesion, Adoption willingess, Increase in understanding [18]
Protection motivation theory (Rogers, 1975)	Perceived severity, perceived vulnerability, perceived response efficacy, perceived self efficacy	[19]–[21], [22], [23]	Trust (only partially)[20] Herd behaviour [19], Gender [22], psychological ownership [23]
Theory of reasoned action (ishbein & Ajzen, 1975)	Attitude, subjective norm	[24]	No added extentions
Theory of planned behaviour (Ajzen, 1991)	Attitude, subjective norm, perceived behavioural control	[13], [25]–[27], [28], [29]	General security awareness (price level not significant) [26], Social influence, usefulness, self-efficacy, facilitating conditions [28], culture [29]
Technology Threat Avoidance Theory [30]	perceived susceptibility, perceived severity, perceived threat, perceived effectiveness, perceived costs, self-efficacy, avoidance motivation, avoidance behaviour, emotion-focused coping.	[31]–[33]	distrust of security, theft of privacy, vulnerability, security threats and security self-efficiacy [32]
Fear Appeal Model [12]	perceived threat severity, threat susceptibility, response efficacy, self efficacy, social influence	[34]	
Technology acceptance model	Perceived ease of use, perceived usefulness	[33], [35]–[38], [13], [21], [24], [39]–[41], [25], [27], [42]	external environment, security budget, prior experience, perceived risks, security planning, confidence in information security and security awareness and training [37] organizational support, personality traits[38] perceived risk [35] security knowledge [39] negatively framed messaging [40]

			security knowledge [24]
			psychological ownership, gender [21],
			technology awareness [27]
			technology specific aspects (biometric)[42]
TOE (Techology – Organization – Environment) framework	Technology, organization, environment	[25], [43]	Cyber catalysts, practice standards [43]
UTAUT (and variants)	Performance expectancy, Effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, habit, behavioural intention	UTAUT [41], [44] UTAUT2 [36], [45], [46]	Trust [46]
Other or no specific framework		[47], [48], [49], [50], [51], [52], [53], [54], [55], [56]	Institutional forces (regulatory, external consultants, other companies), Market forces (consumer concern, size)[47]
			Personal propensity to trust, structural assurance, firm reputation[48]
			awareness, budget, security policy, management support[49]
			social influence, observability [50]
			Economic, organizational, environmental, behavioral/cognitive aspects [51],
			Culture [52],
			Task-Technology fit [53],
			Decisions under uncertainty[54],
			Size, ict use, telework, innovativeness [55],
			Decision-maker overconfidence [56]

4 Discussion

The literature review has identified two main lines of conceptualizing cybersecurity innovation adoption – through the general technology accept theories (mainly TAM, UTAUT, TOE) or through the preventive health models (mainly PMT and TPB). Researchers have frequently found it necessary to extend the base models by including additional constructs relevant for cybersecurity. Several concepts from other disciplines such as psychology and sociology have been used, such as institutional theory,

behavioral/cognitive factors such as culture, trust, social influence, awareness, decision-making under uncertainty and overconfidence. Structural issues, such as size and technology use, as well as the perceived fit between technology and task have also been used.

Of the two main approaches, the preventive health based approach is the approach more conceptually close to cybersecurity risk with its concepts of threats and vulnerabilities. The TAM model of ease-of-use and usability is conceptually easy, and the concept of usability is easily capable of being seen as a formative concept based on different preceding concepts, such as a technology's task-fit and its perceived ability to reduce risk. However several authors find the traditional TAM models lacking in regard to cybersecurity adoption issues [9], [12], and have pointed to the preventive health models as a better theoretical framework because of its inclusion of risk-related constructs. We start by discussing the research based on the general models before moving on to the preventive models.

4.1 Research based on general technology acceptance models

Among the general technology adoption frameworks 14 of the identified studies used the Technology Adoption Model as the main (or a major) theoretical framework, making this the most frequently used framework, trailed by UTAUT/UTAUT2 with 5 studies and TOE with 2 studies among the general technology adoption frameworks. With its concept of ease of use and usefulness, the model is very generic and applicable for many types of technology adoption studies, but its generic nature may also be its weakness, as illustrated by the fact that many studies added new concepts to make the framework more security specific. We summarize some of these studies as follows.

The main additions suggested to the TAM framework were concepts around the perception of risk (perceived risks, security knowledge, general or more specific security technology awareness), organizational aspects (budget, planning, organizational support) and psychological aspects (confidence, ownership, negatively framed messaging).

The UTAUT-based studies rarely added concepts, with the exception of one study on password managers, adding trust as a new concept. The UTAUT framework has received criticism for having too many variables and moderators[57], which may explain a lesser need to extend the framework.

The TOE framework (Technology-Organization-Environment) is also a very generic framework where the TOE aspects are specified for the specific research area. For example, [25] in the organizational adoption phase of their adoption framework, suggest the classical DoI technology factors (relative advantage, complexity, compatibility, visibility and trialability) for the technology concept, for the organization factor top management support, size and security readiness, expertise and culture, and for the environment concept, government regulations and risks of outsourcing. [43] also, through qualitative interviews with IT leaders in various industries, expanded on the TOE framework with cybersecurity specific themes as well as expanding it with two main areas, cyber catalysts (containing cyber risk, privacy, cyber vulnerability), and practice standards (containing ethics, insurance, legal and assessment).

4.2 Preventive models

Among the models with roots in preventive health, the Theory of Planned Behavior with 6 studies and its predecessor, Theory of Reasoned Action with one study was most frequently used. Both these models are quite parsimonious with few, but generic variables (attitude, subjective norm and self-efficacy) that are usually tailored to the specific technology or problem domain they are used in, for example questions specific to cybersecurity knowledge [27], or by adapting the survey questions on attitude, subjective norm etc. directly to the topic (anti-malware or home security software)[24], [26], [28]. The survey questions in these studies may serve as examples to researchers for how to adapt the generic model to the specific research questions.

Protection motivation theory (5 studies) and Health Belief Model (2 studies), with the security relevant concepts of perceived susceptibility/vulnerability and perceived severity/seriousness, perceived benefits/response efficacy, barriers/perceived self-efficacy show how the risk management process of evaluating threats and vulnerabilities affect security adoption decisions. For these studies as well, the survey questions reflecting or forming the concepts were modified from existing scales to be fit for cybersecurity. The main additions to the models are primarily modifiers to the original relationships, such as trust, gender, psychological ownership.

For the Fear Appeals Model, only on study, a replication study performed via Amazon Mechanical Turk, was identified [34] – this replication study found opposite effects for two of five hypothesis in the original study in that they found threat severity to have a positive effect on both response efficacy and self-efficacy, and suggesting that there are differences in the populations in the studies that may explain this, for example familiarity with technology or cultural differences in the samples.

Technology Threat Avoidance Theory, with three identified studies have several common concepts with protection motivation theory, such as perceived susceptibility and perceived severity, perceived effectiveness, perceived costs and self-efficacy, and the main new contribution is the division between problem-oriented and emotional coping behavior. One such emotional coping (or rather, non-coping) mechanism, is capitulation, studied in [32], looking at how experiences with privacy loss and distrust of security leads employees to capitulate when faced with a threat landscape they do not feel capable of managing or contributing to, again leading to a lack of compliance with internal security policies. A division between internal coping mechanisms (self-efficacy) and external coping mechanisms (based on the concepts from TAM) is suggested in [33] to extend the TTAT in a study on acceptance of email authentication services.

4.3 Other approaches to security innovation adoption

In addition to the studies based on the identified major frameworks, 10 studies used some other theoretical framework, or used other approaches such as qualitative or mixed methods to elicit new concepts or constructs relevant to security adoption.

The authors of [47] suggests a research design that uses institutional theory to investigate factors impacting regulatory compliance in the US health care sector, specifically HIPAA compliance, and the effects of institutional forces (regulatory requirements, use

of consultants, other hospitals compliance) and market forces (consumer concern and firms relative size). Institutional theory describes how organizations tend to organize in a similar fashion (isomorphism), mainly driven by three forms of pressure – coercive pressure, for example regulations, laws, cultural expectations in the society they operate, mimetic pressure, when organizations operating under uncertainty, decide to mimic other successful organizations, and normative pressure, often driven through stakeholders, professional organizations and networks that set standards of professionalism an organization is expected to adhere to.

The authors of [49] investigated factors influencing the implementation of information security management systems (ISMS) in universities in Indonesia, and found that awareness, budget, information security policy, and top management support were significant factors. The authors of [52] also investigated the use of ISMS's – specifically ISO27001, but from a cultural perspective – and found higher use of the standard in countries with higher ICT development and discussed cultural aspects such as future orientation, power distance and low institutional collectivism to explain this difference.

The authors of [46] investigated the intention to use password managers based on initial trust of the technology based on the Initial Trust Model from [58]. The study found that initial trust, as based on the concepts of structural assurances (guarantees of technical measures, certifications etc) and firm reputation were found to significantly relate to initial trust (but not the users personal propensity to trust), and initial trust had a significant effect on the intention to adopt password managers.

In [50] the role of social influence in the adoption of security measures, specifically three Facebook security features, were investigated. The study suggested that social influence (the effect of peers, friends adoption) affects security feature adoption, but this was moderated by both the technologies individual attributes, the overall adoption among friends as well as the number of distinct social spheres the friends originate from.

The authors of [51] highlights that traditional, cost based risk analyses does not adequately address the factors that contribute to cybersecurity investment decisions, and neglects the importance of economic, organizational, environmental and behavioral/cognitive aspects. Based on a series of expert interviews, they elaborated on some of these themes and conducted a literature survey on decisions around security investments. Also highlighting cognitive aspects, [56] investigated how the overconfidence of executives affect information security investments and posits that existing models are overly reliant on the decision makers rational behavior. They found through a survey that overconfidence had a negative effect on security investments.

The authors of [55] suggested a theoretical model for the adoption of a security technology, InfoCards, based on the Task-Technology Fit model [59] a research model that seeks to explain technology adoption based on the fit between the task to be performed and the technology. The task and technology factors that make up the concept of "fit" needs to be tailored to the specific area/technology under adoption, but the authors also suggest TAM as a model that should be integrated. In a similar way, [55] investigated the adoption of PKI as a security technology in European firms, the study found high use of ICT, telework, company innovativeness and size to be factors contributing to the adoption.

With a behavioral economics approach, [54] investigated the adoption of security products as a process of decision under uncertainty, the uncertainty being related to the environment (knowledge of threats) and the product (level of information about the effectiveness of the product), and suggested an experiment to evaluate this model.

4.4 Adoption in an organizational context

Several of the diffusion and acceptance models focus on adoption and acceptance in voluntary context and as a personal choice – something which is often less relevant in an organizational context where choice of technologies is more dependent on managerial and organizational decision processes, organizational strategies, acquisition processes and financial investment choices. In this setting, the individual employee might have less of a say in what innovations are adopted, but their role in the implementation of the innovation is crucial to the final outcome or success of the total innovation process.

In an organizational setting the adoption process is generally divided in three stages - initiation (pre-adoption), adoption-decision and implementation (post-adoption). In the organizational context the first two phases may be said to mostly follow and be influenced by organizational policies and practices and is therefore best understood by frameworks focusing on organizational adoption, while the implementation and post-adoption phase is to a larger extent dependent on individual behavior and thereby better understood by more individually oriented frameworks such as TAM and TPB. This is also supported by [2] that reviewed 151 innovation adoption studies, and found the DoI framework and the TOE framework to be the most frequently used framework for organizational level adoption studies, while TAM, TRA, TPB were most frequently used to study adoption on an individual level.

The difference between organizational and individual adoption, and the stagewise process from decision to implement to actual organizational user acceptance is also discussed in [60], which suggest that traditional Diffusion of Innovation models fall short when it comes to explaining adoption in organizational settings where users are mandated to use the technology, or where there is a high need for knowledge or coordinated action to implement the technology or the implementation. Hameed and Arachchilage [25] also suggest a two-phased model of IS security innovation where the organizational adoption is described by factors from the TOE framework, while the user acceptance phase is determined by user attitude, subjective norms, perceived behavioral control, computer self-efficacy, perceived usefulness, perceived ease of use and image, concepts largely found in the UTAUT framework.

5 Further work

As illustrated, a range of theories and frameworks have been used to explain cybersecurity adoption decisions, and no unified framework exists. While the parsimonious models from the general technology adoption models and the preventive health based models have had success in explaining adoption on an individual level, research on

organizational adoption have utilized more complex models like TOE, but at the cost of predictive power and more quantitative measures on the effect of the various drivers. Further work should focus on developing more quantitative measures, first by identifying good measures for organizational cybersecurity innovations, and identifying relevant metrics to measure the effect of these concepts. While several frameworks have been suggested to build metrics for cybersecurity maturity, like certification schemes such as ISO 27001, or capability maturity models like the NIST Cybersecurity Framework CSF, or C2M2), these frameworks are extensive and time consuming, and the reliability at times questionable. To operationalize the concept of cybersecurity adoption, the scoring of the number of implemented technical cybersecurity controls from a set of validated advanced capabilities, technologies not in general use, as judged from the complexity scores from relevant cybersecurity frameworks that rate complexity to implement (like the Critical Security Controls) , as well as from a set of cybersecurity experts with practical knowledge of control implementation across a large set of organizations, may be suggested as one measure of cybersecurity innovation adoption.

Further research should also focus on measuring the effect of other factors identified from the survey to evaluate the effect of concepts such as perceived severity and perceived vulnerability (organizational threat assessments), the effects of social norms, for example in the context of knowledge sharing networks often suggested for sectors and industries. More research should also be done to identify the suitability of different models for different use cases, and how the effect of the different constructs may vary according to the situation the model is applied to.

6 Conclusion

Several approaches to describe and model the adoption of cybersecurity innovations, and our literature review identified two main approaches – the Technology adoption model based approaches, and the behavioral health based approaches. Most of the identified studies focused on the adoption of a single technology, and many discuss adoption in a voluntary, non-organizational setting, but collectively they contribute to a better understanding of factors driving cybersecurity technology adoption from various viewpoints.

Based on the literature review, we have identified several relevant factors to study cybersecurity innovation adoption in an organizational setting, and suggest how these concepts may be used in later research to build better models for technological adoption of cybersecurity innovations.

7 Acknowledgements

This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105

8 References

1. E. M. Rogers, *Diffusion of innovations*. New York, NY: Free Press, 2003.
2. M. A. Hameed, S. Counsell, and S. Swift, "A conceptual model for the process of IT innovation adoption in organizations," *Journal of Engineering and Technology Management*, vol. 29, no. 3, pp. 358–390, Jul. 2012, doi: 10.1016/j.jengtecman.2012.03.007.
3. F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, vol. 35, no. 8, pp. 982–1003, 1989.
4. V. Venkatesh and F. D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science*, vol. 46, no. 2, pp. 186–204, Feb. 2000, doi: 10.1287/mnsc.46.2.186.11926.
5. I. Ajzen and M. Fishbein, *Understanding attitudes and predicting social behavior*, Pbk. ed. Englewood Cliffs, N.J.: Prentice-Hall, 1980.
6. I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, Dec. 1991, doi: 10.1016/0749-5978(91)90020-T.
7. V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," May 2008, doi: 10.1111/j.1540-5915.2008.00192.x.
8. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, 2003, doi: 10.2307/30036540.
9. V. Venkatesh, J. Y. L. Thong, and X. Xu, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly*, vol. 36, no. 1, pp. 157–178, 2012, doi: 10.2307/41410412.
10. L. G. Tornatzky, M. Fleischer, and A. K. Chakrabarti, *The processes of technological innovation*. in Issues in organization and management series. Lexington, Mass: Lexington Books, 1990.
11. J. Baker, "The Technology–Organization–Environment Framework," in *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1*, Y. K. Dwivedi, M. R. Wade, and S. L. Schneberger, Eds., in Integrated Series in Information Systems. New York, NY: Springer, 2012, pp. 231–245. doi: 10.1007/978-1-4419-6108-2_12.
12. A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *Management Information Systems Quarterly*, vol. 34, no. 3, pp. 549–566, 2010.
13. T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *JAIS*, vol. 8, no. 7, pp. 386–408, Jul. 2007, doi: 10.17705/1jais.00133.
14. R. West, "The psychology of security," *Commun. ACM*, vol. 51, no. 4, pp. 34–40, Apr. 2008, doi: 10.1145/1330311.1330320.
15. J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, vol. 19, no. 5, pp. 469–479, Sep. 1983, doi: 10.1016/0022-1031(83)90023-9.
16. I. M. Rosenstock, "Historical Origins of the Health Belief Model," *Health Education Monographs*, vol. 2, no. 4, pp. 328–335, Dec. 1974, doi: 10.1177/109019817400200403.
17. D. Wynn, C. Williams, E. Karahanna, and R. Madupalli, "Preventive Adoption of Information Security Behaviors," *ICIS 2013 Proceedings*, 2013, [Online]. Available: https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/5
18. B. Pickering, C. Boletsis, R. Halvorsrud, S. Phillips, and M. Surridge, "It's Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness," in *HCI for*

Cybersecurity, Privacy and Trust, A. Moallem, Ed., in Lecture Notes in Computer Science, vol. 12788. Cham: Springer International Publishing, 2021, pp. 337–352. doi: 10.1007/978-3-030-77392-2_22.

19. A. Vedadi and M. Warkentin, "Can Secure Behaviors Be Contagious? A Two-Stage Investigation of the Influence of Herd Behavior on Security Decisions," *Journal of the Association for Information Systems*, vol. 21, no. 2, 2020, [Online]. Available: https://aisel.aisnet.org/jais/vol21/iss2/3
20. R. Ayyagari, J. Lim, and O. Hoxha, "Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers," *CMR*, vol. 15, no. 4, pp. 227–245, Dec. 2019, doi: 10.7903/cmr.19394.
21. K. K. W. Ho, C. H. (Allen) Au, and D. K. W. Chiu, "Home Computer User Security Behavioral Intention: A Replication Study from Guam," *AIS Transactions on Replication Research*, vol. 7, no. 1, 2021, [Online]. Available: https://aisel.aisnet.org/trr/vol7/iss1/4
22. R. Sonnenschein, A. Loske, and P. Buxmann, *Gender Differences in Mobile Users' IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study*. 2016. [Online]. Available: https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/12
23. C. Smith and R. Agarwal, "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *Management Information Systems Quarterly*, vol. 34, no. 3, pp. 613–643, Sep. 2010.
24. Ping An Wang, "Information security knowledge and behavior: An adapted model of technology acceptance," in *2010 2nd International Conference on Education Technology and Computer*, Shanghai, China: IEEE, Jun. 2010, pp. V2-364-V2-367. doi: 10.1109/ICETC.2010.5529366.
25. M. A. Hameed and N. A. G. Arachchilage, "A Model for the Adoption Process of Information System Security Innovations in Organisations: A Theoretical Perspective," *ACIS 2016 Proceedings*, 2016, [Online]. Available: https://aisel.aisnet.org/acis2016/45
26. A. Vafaei-Zadeh, R. Thurasamy, and H. Hanifah, "Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior," *K*, vol. 48, no. 8, pp. 1565–1585, Sep. 2019, doi: 10.1108/K-05-2018-0226.
27. T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention Toward Preventive Technologies in the Context of Voluntary Use," *SIGHCI 2005 Proceedings*, 2005, [Online]. Available: https://aisel.aisnet.org/sighci2005/10
28. B.-Y. Ng and M. Rahim, "A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security," *PACIS 2005 Proceedings*, 2005, [Online]. Available: https://aisel.aisnet.org/pacis2005/20
29. T. Dinev, J. Goo, Q. Hu, and K. Nam, "User behavior toward preventive technologies – cultural differences between the United States and South Korea," *ECIS 2006 Proceedings*, 2006, [Online]. Available: https://aisel.aisnet.org/ecis2006/9
30. H. Liang and Y. Xue, "Avoidance of Information Technology Threats: A Theoretical Perspective," *Management Information Systems Quarterly*, vol. 33, no. 1, pp. 71–90, 2009.
31. D. K. Young, D. Carpenter, and A. McLeod, "Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication," *AIS Transactions on Replication Research*, vol. 2, no. 1, 2016, [Online]. Available: https://aisel.aisnet.org/trr/vol2/iss1/8
32. A. McLeod and D. Dolezel, *Toward Security Capitulation Theory*. 2020. [Online]. Available: https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/2
33. T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service: Security services as coping mechanisms," *Information Systems Journal*, vol. 24, no. 1, pp. 61–84, Jan. 2014, doi: 10.1111/j.1365-2575.2012.00420.x.

34. S. Samtani, H. Zhu, and S. Yu, “Fear Appeals and Information Security Behaviors: An Empirical Study on Mechanical Turk,” *AIS Transactions on Replication Research*, vol. 5, no. 1, 2019, [Online]. Available: https://aisel.aisnet.org/trr/vol5/iss1/5
35. R. Groner and P. Brune, “Towards an Empirical Examination of IT Security Infrastructures in SME,” in *Secure IT Systems*, A. Jøsang and B. Carlsson, Eds., in Lecture Notes in Computer Science, vol. 7617. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 73–88. doi: 10.1007/978-3-642-34210-3_6.
36. L. Tafokeng Talla and J. R. Kala Kamdjoug, “Factors Influencing Adoption of Information Security in Information Systems Projects,” in *New Knowledge in Information Systems and Technologies*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds., in Advances in Intelligent Systems and Computing, vol. 931. Cham: Springer International Publishing, 2019, pp. 890–899. doi: 10.1007/978-3-030-16184-2_84.
37. P. Seuwou, E. Banissi, and G. Ubakanma, “User Acceptance of Information Technology: A Critical Review of Technology Acceptance Models and the Decision to Invest in Information Security,” in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*, H. Jahankhani, A. Carlile, D. Emm, A. Hosseinian-Far, G. Brown, G. Sexton, and A. Jamal, Eds., in Communications in Computer and Information Science, vol. 630. Cham: Springer International Publishing, 2016, pp. 230–251. doi: 10.1007/978-3-319-51064-4_19.
38. J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior,” *Computers & Security*, vol. 49, pp. 177–191, Mar. 2015, doi: 10.1016/j.cose.2015.01.002.
39. S. M. Lui and W. Hui, “The effects of knowledge on security technology adoption: Results from a quasi-experiment,” in *The 5th International Conference on New Trends in Information Science and Service Science*, Oct. 2011, pp. 328–333.
40. J. D. Shropshire, M. Warkentin, and A. C. Johnston, “Impact of Negative Message Framing on Security Adoption,” *Journal of Computer Information Systems*, vol. 51, no. 1, pp. 41–51, Sep. 2010, doi: 10.1080/08874417.2010.11645448.
41. M. Warkentin, J. Shropshire, and A. Johnston, “The IT Security Adoption Conundrum: An Initial Step Toward Validation of Applicable Measures,” *AMCIS 2007 Proceedings*, 2007, [Online]. Available: https://aisel.aisnet.org/amcis2007/276
42. G. Ho, G. Stephens, and R. Jamieson, “Biometric Authentication Adoption Issues,” *ACIS 2003 Proceedings*, 2003, [Online]. Available: https://aisel.aisnet.org/acis2003/11
43. S. Wallace, K. Y. Green, C. Johnson, J. Cooper, and C. Gilstrap, “An Extended TOE Framework for Cybersecurity-adoption Decisions,” *Communications of the Association for Information Systems*, vol. 47, no. 1, 2020, [Online]. Available: https://aisel.aisnet.org/cais/vol47/iss1/51
44. W. W. Lidster and S. S. M. Rahman, “Identifying Influences to Information Security Framework Adoption: Applying a Modified UTAUT,” in *2020 IEEE International Conference on Big Data (Big Data)*, Atlanta, GA, USA: IEEE, Dec. 2020, pp. 2605–2609. doi: 10.1109/BigData50022.2020.9378283.
45. M. Alqahtani and R. Braun, “Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review,” *JIACS*, vol. 2021, pp. 1–15, May 2021, doi: 10.5171/2021.666987.
46. R. Maclean and J. Ophoff, “Determining Key Factors that Lead to the Adoption of Password Managers,” in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, Plaine Magnien: IEEE, Dec. 2018, pp. 1–7. doi: 10.1109/ICONIC.2018.8601223.

47. A. Appari, M. E. Johnson, and D. L. Anthony, “HIPAA Compliance: An Institutional Theory Perspective,” *AMCIS 2009 Proceedings*, 2009, [Online]. Available: https://aisel.aisnet.org/amcis2009/252
48. A. Farooq, A. Dubinina, S. Virtanen, and J. Isoaho, “Understanding Dynamics of Initial Trust and its Antecedents in Password Managers Adoption Intention among Young Adults,” *Procedia Computer Science*, vol. 184, pp. 266–274, 2021, doi: 10.1016/j.procs.2021.03.036.
49. P. K. Sari, N. Nurshabrina, and Candiwan, “Factor analysis on information security management in higher education institutions,” in *2016 4th International Conference on Cyber and IT Service Management*, Bandung, Indonesia: IEEE, Apr. 2016, pp. 1–5. doi: 10.1109/CITSM.2016.7577518.
50. S. Das, A. D. I. Kramer, L. A. Dabbish, and J. I. Hong, “The Role of Social Influence in Security Feature Adoption,” in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, Vancouver BC Canada: ACM, Feb. 2015, pp. 1416–1426. doi: 10.1145/2675133.2675225.
51. M. Heidt, J. Gerlach, and P. Buxmann, *A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions*. 2019. [Online]. Available: https://aisel.aisnet.org/hicss-52/os/information_security/5
52. M. Mirtsch, J. Pohlisch, and K. Blind, “International Diffusion of the Information Security Management System Standard ISO/IEC 27001: Exploring the Role of Culture,” *ECIS 2020 Research Papers*, 2020, [Online]. Available: https://aisel.aisnet.org/ecis2020_rp/88
53. A. Alkhalifah and J. D’Ambra, “Applying Task-Technology Fit to the Adoption of Identity Management Systems,” *ACIS 2011 Proceedings*, 2011, [Online]. Available: https://aisel.aisnet.org/acis2011/31
54. K. S. Egorova, “Adoption of Information Security as Decision-making under Uncertainty: A Behavioural Economics Approach,” *ECIS 2015 Research-in-Progress Papers*, 2015, [Online]. Available: https://aisel.aisnet.org/ecis2015_rip/21
55. E. Loukis, S. Kokolakis, and K. Anastasopoulou, “Factors of PKI adoption in European firms,” in *MCIS 2011 Proceedings*, 2011. [Online]. Available: https://aisel.aisnet.org/mcis2011/29
56. K. Dong, R. Lin, X. Yin, and Z. Xie, “How does overconfidence affect information security investment and information security performance?,” *Enterprise Information Systems*, vol. 15, no. 4, pp. 474–491, Apr. 2021, doi: 10.1080/17517575.2019.1644672.
57. R. P. Bagozzi, “The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift.,” *Journal of the Association for Information Systems*, vol. 8, no. 4, Apr. 2007, doi: 10.17705/1jais.00122.
58. D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and Validating Trust Measures for e-Commerce: An Integrative Typology,” *Information Systems Research*, vol. 13, no. 3, pp. 334–359, Sep. 2002, doi: 10.1287/isre.13.3.334.81.
59. D. L. Goodhue and R. L. Thompson, “Task-Technology Fit and Individual Performance,” *MIS Quarterly*, vol. 19, no. 2, pp. 213–236, 1995, doi: 10.2307/249689.
60. M. J. Gallivan, “Organizational adoption and assimilation of complex technological innovations: development and application of a new framework,” *SIGMIS Database*, vol. 32, no. 3, pp. 51–85, Jul. 2001, doi: 10.1145/506724.506729.