

The HORM Diagramming Tool: A Domain-Specific Modelling Tool for SME Cybersecurity Awareness

Costas Boletsis¹ ^a, Sefat Noor Orni² and Ragnhild Halvorsrud¹ ^b

¹*SINTEF Digital, Oslo, Norway*

²*Department of Informatics, University of Oslo, Oslo, Norway*
fi

Keywords: CJML, Cybersecurity, Modelling, User Journey, Visualisation.

Abstract: Improving security posture while addressing human errors made by employees are among the most challenging tasks for SMEs concerning cybersecurity risk management. To facilitate these measures, a domain-specific modelling tool for visualising cybersecurity-related user journeys, called the HORM Diagramming Tool (HORM-DT), is introduced. By visualising SMEs' cybersecurity practices, HORM-DT aims to raise their cybersecurity awareness by highlighting the related gaps, thereby ultimately informing new or updated cyber-risk strategies. HORM-DT's target group consists of SMEs' employees with various areas of technical expertise and different backgrounds. The tool was developed as part of the Human and Organisational Risk Modelling (HORM) framework, and the underlying formalism is based on the Customer Journey Modelling Language (CJML) as extended by elements of the CORAS language to cover cybersecurity-related user journeys. HORM-DT is a fork of the open-source Diagrams.net software, which was modified to facilitate the creation of cybersecurity-related diagrams. To evaluate the tool, a usability study following a within-subject design was conducted with 29 participants. HORM-DT achieved a satisfactory system usability scale score of 80.69, and no statistically significant differences were found between participants with diverse diagramming tool experience. The tool's usability was also praised by participants, although there were negative comments regarding its functionality of connecting elements with lines.

1 INTRODUCTION

Small and medium enterprises (SMEs) are increasingly being exposed to cyber-risks. In 2017 alone, 61% of SMEs were exposed to malware cyberattacks (Khan et al., 2020). Despite their increasing exposure to cyberattacks, SMEs rarely conduct thorough cyber-risk assessments, and more than half of them provide either an outdated or no cyber-risk strategy at all (Benz and Chatterjee, 2020; Paulsen, 2016; The National Center for the Middle Market, 2016; Boletsis et al., 2021). This may be due to internal issues that arise when attempting to set up cyber-risk strategies, such as 'having small IT teams, inadequate security budgets, and disagreements between IT and business leadership teams regarding cybersecurity risk management' (Boletsis et al., 2021). It has been reported that the most challenging tasks for cybersecurity risk management in SMEs are i) defining

and taking the first step towards improving their security posture and ii) addressing human errors made by employees, which is the 'human element' sometimes referred to as the biggest internal threat for SMEs (Arctic Wolf, 2017; Meshkat et al., 2020; Symantec, 2019; Boletsis et al., 2021).

To address the first challenge, it has been suggested that mapping SMEs' current practices and the potential threats they face would be a useful initial move in cybersecurity risk management (Benz and Chatterjee, 2020; Paulsen, 2016; Meszaros and Buchalcevova, 2017). This mapping should also address the second big challenge by modelling the human element in cybersecurity-related scenarios, essentially through the documentation of user journeys related to cybersecurity, which are the visual paths that users may take when performing an action or using a service (Stickdorn et al., 2018; Boletsis et al., 2021). At the same time, end-users/employees should be involved in the modelling process, always taking into consideration their diverse technical backgrounds (Paulsen, 2016; Kullman et al., 2020; Bellamy et al.,

^a  <https://orcid.org/0000-0003-2741-8127>

^b  <https://orcid.org/0000-0002-3774-4287>

2007; Boletsis et al., 2021).

This paper presents, the HORM Diagramming Tool (HORM-DT)¹, a domain-specific modelling tool for visualising cybersecurity-related user journeys, and evaluates its usability. The tool's main target group consists of SME employees with various areas of technical expertise and different backgrounds, and so usability is of the essence. By using the tool and the models produced by it, the aim is to raise cybersecurity awareness so that SMEs can visualise their practices and the potential cyber threats they face and identify the gaps. In this way, they can develop up-to-date or new cyber-risk strategies in an informed way.

The tool was developed as part of the Human and Organizational Risk Modelling (HORM) framework² to be a comprehensible and easy-to-use cybersecurity-related framework for capturing the risks that ordinary people may be exposed to (Fair et al., 2022). HORM is based on the Customer Journey Modelling Language (CJML) (Halvorsrud et al., 2021) and extended by formalism from the CORAS language (Lund et al., 2011; Vraalsen et al., 2005) so that it can address cybersecurity-related user journeys.

2 RELATED WORK

When conducting cybersecurity assessments, simply providing accurate risk information may not be enough to ensure that individuals will be able to comprehend a risk message and act on it (Nurse et al., 2011; Slovic, 1999; Skubisz et al., 2009; Boletsis et al., 2021). However, visualisations can be an important factor in communicating cyber risks (Boletsis et al., 2021). In the field of SME cybersecurity awareness, a limited number of works have evaluated SMEs' cybersecurity practices by utilising visual elements (Boletsis et al., 2021), including the following:

- CYSEC, a do-it-yourself cybersecurity assessment method for SMEs that automates elements of a counselling dialogue between a security expert and employees in the SME to counter cyber threats (Shojaifar, 2019).
- The SME Cybersecurity Evaluation Tool, which consists of a 35-question online survey to be completed by IT leaders to self-rate their maturity based on the National Institute of Standards and Technology cybersecurity framework (Benz and Chatterjee, 2020).

¹HORM-DT can be accessed at: <https://cjml.no/horm2/> and its code is available from the Github repository at: <https://github.com/CostasBoletsis/HORM-DT>

²HORM website: <https://cjml.no/horm/>

- The System Security Modeller (SSM), which is an asset-based risk-analysis tool that provides an information security perspective to the interactions between assets across an entire system and can be also applied in SME settings (Boletsis et al., 2021; Surridge et al., 2019).
- A gamified approach for raising awareness surrounding SMEs' level of cybersecurity and resilience (Ponsard and Grandclaudon, 2019), for which SME employees answer a cybersecurity quiz and a self-assessment questionnaire.

It can be said that these approaches for mapping SMEs' cybersecurity practices focus more on representations of infrastructure than on human actors and their behaviours. At the same time, 'there is no holistic visualisation approach that could facilitate information distribution between employees of different levels of expertise' (Boletsis et al., 2021).

Each SME process essentially represents a pathway through a sequence of events. The modelling and visualisation of these processes could be covered by user journey modelling languages (Boletsis et al., 2021). To that end, the HORM framework was developed (Fair et al., 2022).

The HORM framework focuses on the 'human element' and its modelling, and it consists of a modelling language, based on a version of the CJML (Haugstveit et al., 2016; Halvorsrud et al., 2016a; Halvorsrud et al., 2014; Halvorsrud et al., 2016b) extended through contributions from the CORAS language to fulfil cybersecurity-related purposes, and a set of tools for modelling.

CJML is a visual language for the modelling and visualisation of service and work processes in terms of customer or user journeys (Halvorsrud et al., 2021; Boletsis et al., 2021). Being centred on humans and their activities, CJML appeals to a broad user group through its simple and intuitive form (Halvorsrud et al., 2016a), a feature that is attributed to the user-centred design methodology that led its design. The basic units of CJML are observable touchpoints that can take the form of a *communication event* or a *non-communicative activity or action*. In CJML, the sequence of touchpoints that a user follows to achieve a specific goal constitutes a *user journey*. There are two types of diagram available in CJML that serve different purposes (Figure 1). The simple *journey diagram* is suitable for journeys with few actors and emphasises any deviation from the planned journey. The *swimlane diagram* is useful for journeys involving several actors and emphasises both the initiator and the recipient of a touchpoint (Halvorsrud et al., 2021; Halvorsrud et al., 2016a).

CJML has been extended to model cybersecurity-

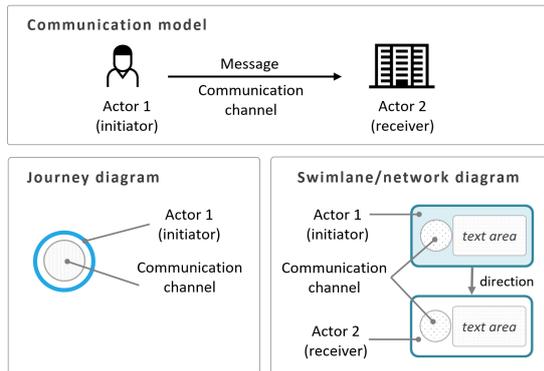


Figure 1: CJML’s communication model with a sender transmitting a message to a receiver through a communication channel (upper part). The visual representation of a touchpoint in the case of a journey diagram (left) and a swimlane diagram (right) (Boletsis et al., 2021).

related user journeys using elements from the CORAS language. CORAS is ‘a model-driven approach to risk analysis that consists of a method, a language and a tool to support the risk analysis process’ (Lund et al., 2011). The CORAS graphical language, an extension of the Unified Modelling Language (UML) 2.0 specification language, allows for ‘documentation of undesirable behaviour in the form of threat scenarios’ (Vraalsen et al., 2005). In the CORAS language, a *threat* is described as ‘using a threat agent, e.g., a disloyal employee or a computer virus. The threat agent initiates a threat scenario, which is a sequence of events or activities leading to an *unwanted incident*, i.e., an event resulting in a reduction in the value of the target asset’ (Vraalsen et al., 2005). These two new elements of *threats* and *unwanted incidents* have been added in both CJML formalism and its concrete syntax as icons (Figure 2). Moreover, the CJML users and ‘deviations’ were redefined to fit the cybersecurity context, such that the users are SME employees and external users that make use of SME infrastructure under business-to-business (B2B) offerings, and the ‘deviations’ are the cyber threats (Boletsis et al., 2021).

Within the HORM cybersecurity-related context, CJML has been applied using MS PowerPoint tem-



Figure 2: The icons of *threat* and *unwanted incident* that were integrated from CORAS to CJML to extend CJML and address cybersecurity-related user journeys.

plates as its tool³. Therefore, rather than relying on third-party software, there is room and a need for the development of a standalone modelling and diagramming tool to act as a user interface (UI) for the extended CJML (i.e., HORM) modelling language (Figure 3). At the same time, UI usability is important, and having a standalone, independent modelling tool would enable developers to tweak the tool and its source code until they reach satisfactory levels of UI usability.

3 HORM DIAGRAMMING TOOL

3.1 Development

HORM-DT was developed using the open-source Diagrams.net (previously Draw.io) graph drawing software by JGraph⁴ (Figure 3), developed in HTML5 and JavaScript. The interface of the Diagrams.net open-source software enables the user to easily create and manage diagrams such as flowcharts, wireframes, organisational charts and network diagrams⁵. Its main features include the creation of a wide range of diagrams, the availability of templates for diagrams, display relationships between objects using various types of graph element (such as shapes, arrows, text, images and icons), the import of images/icons from external sources and the storage and export of created diagrams in several image formats and other formats, such as XML, PDF, HTML and more (JGraph, 2022). The Diagrams.net open-source software was

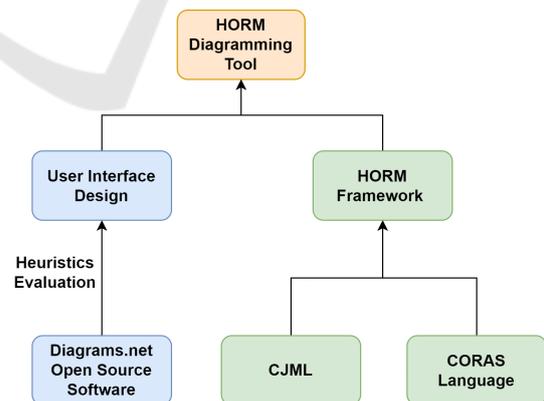


Figure 3: The UI and modelling formalism components that were utilised for the creation of HORM-DT.

³MS PowerPoint templates for the extended CJML: https://cjml.no/horm/CJML_Diagram_generator.v1.pptx

⁴Code repository of the open-source Diagrams.net software: <https://github.com/jgraph/drawio>

⁵Diagrams.net website: <https://diagrams.net/>

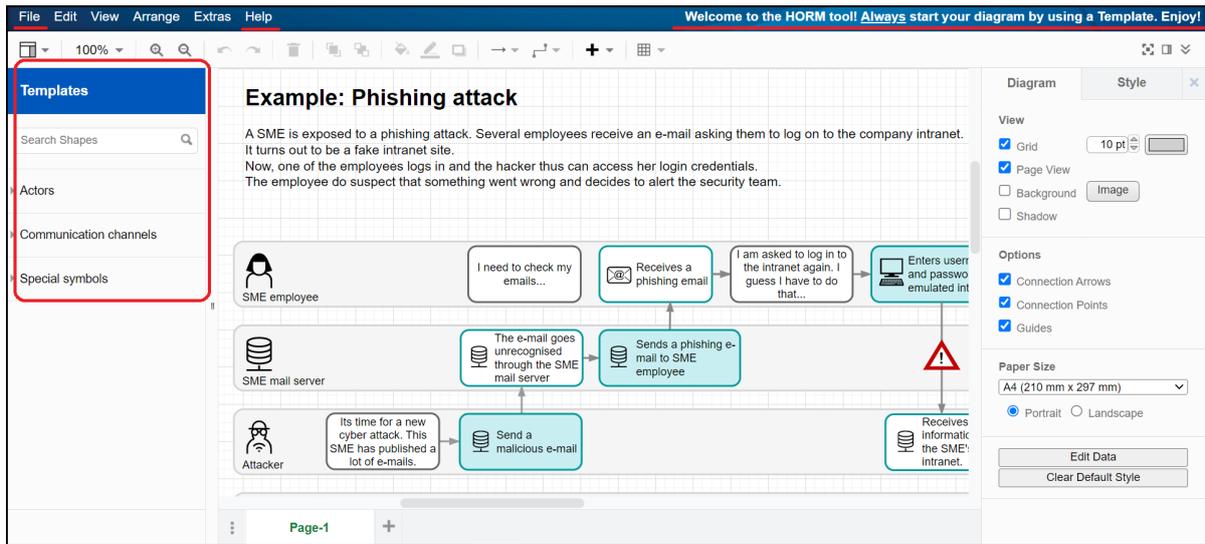


Figure 4: A screenshot of the HORM-DT UI with the tweaked interface areas, based on a heuristic evaluation, highlighted in red. HORM-DT can be accessed at <https://cjml.no/horm2/>

considered and used because i) it is widely popular among software engineers (Rauer, 2019; Von Der Assen et al., 2022) and ii) it was presented, analysed, and/or used in several studies regarding modelling languages and tools (Von Der Assen et al., 2022; Jaimez-González and Martínez-Samora, 2020; Agárdi, 2022; Vakaliuk et al., 2021; Chávez-Feria et al., 2022; Chávez-Feria et al., 2021).

3.2 User Interface Design

Although the Diagrams.net software comes with an already designed UI, a heuristic evaluation of it was of the essence because HORM-DT should address users of all technical backgrounds (Figure 3). The heuristic evaluation was conducted in an informal manner by the authors, who utilised the ten usability heuristics for UI design (Nielsen, 2020). The UI design inherited from the Diagrams.net software fulfilled almost all heuristics; however, the following few tweaks were made to further address the specific nature and domain of our tool:

- **Templates:** Based on the CJML formalism, a user journey modelling process should start by using a template that contains the basic elements of the concrete syntax. To that end, templates for swimlane and journey diagrams, as well as examples of models, were added and made accessible right from the landing page. At the same time, a distinctive ‘Templates’ menu button was added to the left-hand side icon library (Figure 4) so that users can access the templates at any point, thereby addressing the heuristic of providing ‘user control and freedom’ (Nielsen, 2020). A text message at

the top of the UI was inserted (Figure 4) to remind users about always using a template when starting to design a cybersecurity-related diagram (addressing the ‘error prevention’ heuristic; Nielsen, 2020).

- **Icon Library:** The icon library at the left-hand side of the UI (Figure 4) was redesigned and simplified in relation to the one ‘inherited’ from the Diagrams.net software. Icon groups of various other charts included in Diagrams.net, such as network charts, flowcharts, tables, wireframes and business charts, were removed, since they did not comply with the tool’s cybersecurity-related intended use. That way, a more focused, minimalist design approach was followed (addressing the ‘aesthetic and minimalist design’ heuristic; Nielsen, 2020) with the aim of minimising users’ cognitive load by enabling them to focus only on icons defined by the CJML concrete syntax under the icon categories of Actors, Communication channels and Special symbols (addressing the ‘recognition rather than recall’ heuristic; Nielsen, 2020). Naturally, users are still able to create simple shapes, such as squares and circles, by using the search function or the ‘+’ symbol on the horizontal toolbar.
- **Saving and Exporting Diagrams:** Users can save their diagrams in the native Draw.io, XML-based format and can also export them in various image and document formats. The saving and export functionalities are located under the ‘File’ drop-down menu (Figure 4). Diagrams.net software, by default, enables saving diagrams lo-

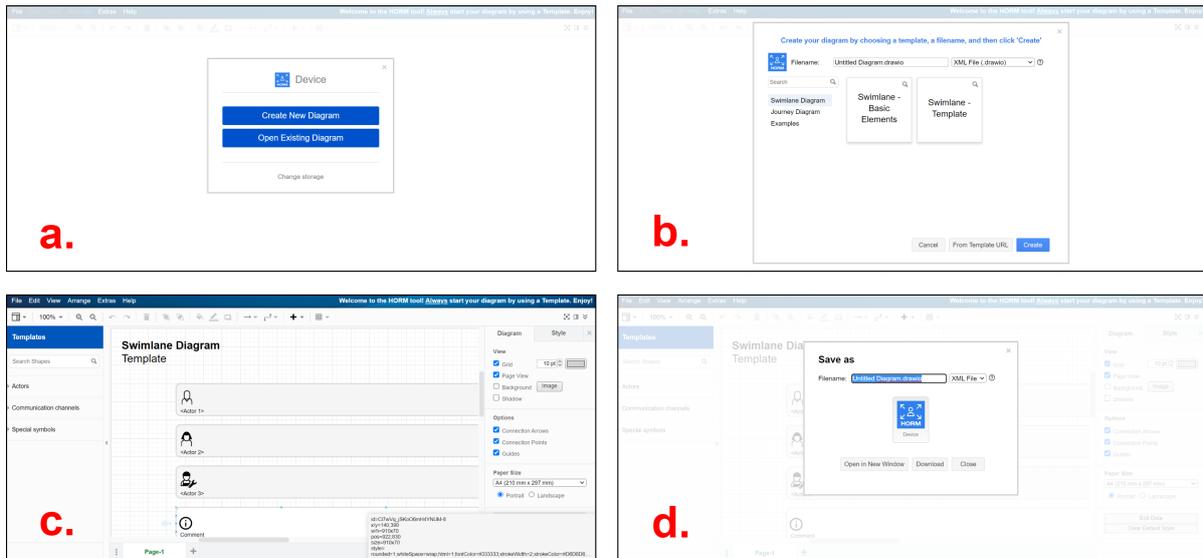


Figure 5: Four screenshots presenting the UI of HORM-DT: a) the landing page, b) the ‘Templates menu’, c) the canvas and d) the ‘Save as’ box.

cally and on connected, commercial cloud storage providers, such as Google Drive and MS OneDrive. Since these storage options belong to commercial platforms (Von Der Assen et al., 2022), which users may or may not use, their integration was excluded, and only saving/exporting to the local drive was provided as an option; that way, confusing users by suddenly introducing various storage options when saving/exporting could be avoided (addressing the ‘consistency’-related heuristic; Nielsen, 2020).

- **Help and Guidance:** The ‘Help’ dropdown menu (Figure 4) was edited so that it provides users guidance on the use of the tool and information on the HORM framework. This change addressed the ‘help and documentation’ heuristic (Nielsen, 2020).

3.3 Use

The basic functionalities of HORM-DT are presented as follows:

- On the landing page, users can choose whether to load a previously saved diagram or to create a new one (Figure 5a).
- Upon making the choice of creating a new diagram, users are asked to choose a template (Figure 5b). Templates can contain just the elements of the HORM formalism or come with guidance about what each symbol represents and how it is used. Upon choosing a template, a canvas appears on which users can work and create models using

icons, shapes, text and arrows (Figure 5c).

- When users want to save the model they have created, there are two options. They can save the model locally as a diagram file in the software’s native XML-based format (Figure 5d), or they can export it in the format of their choice (image or document).

4 EVALUATION

4.1 Methodology

For the evaluation of HORM-DT, the focus was on the tool’s perceived usability. Since the CJML formalism and the CORAS framework have been validated in a number of past user studies (Halvorsrud et al., 2016a; Halvorsrud et al., 2021; Stølen, 2001; Stølen et al., 2002; Dimitrakos et al., 2002; Raptis et al., 2002), the main purpose of this work was to evaluate the new UI elements and investigate the extent to which HORM-DT (i.e., a diagramming tool based on the Diagrams.net software) can facilitate user interaction with the concrete syntax and the model creation under the HORM-related formalism. A common way of conducting the evaluation of modelling languages and tools is to provide participants with textual descriptions of scenarios/cases and ask of them to turn them into models using the respective languages and tools (Silva et al., 2018; Miranda et al., 2018). In this work, and since the focus was exclusively on the tool, the participants were provided with the visual representations of cybersecurity-related user journeys,

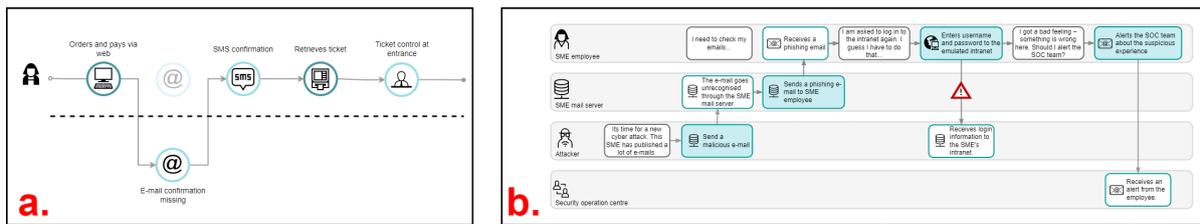


Figure 6: a) A HORM model of an online-service user journey with a problematic point/deviation, which had to be reproduced by the study participants as the first, introductory task. b) A HORM model of a phishing attack against an SME employee that had to be reproduced by the study participants as the second, main task.

namely ready-made models, and asked to reproduce them using HORM-DT. Therefore, the participants were asked to use and evaluate the UI of HORM-DT without needing to ‘speak’ HORM’s modelling language.

The evaluation study took place between March and June 2022 and followed a within-subject design. Moreover, a within-subject comparison took place between the participants with prior experience with diagramming tools (hereafter called ‘experienced’) and those without (‘inexperienced’).

4.2 Participants

The participants were recruited from the authors’ institutions, and the majority were students from the University of Oslo. Prior knowledge of cybersecurity and experience using diagramming tools were not required. All the participants provided informed consent to participate in the study.

4.3 Measures

The study deployed a mixed-methods research design utilising qualitative and quantitative measures.

Demographic data were collected in the initial stage of the study. A demographic questionnaire collected information on age, gender, whether participants had previous experience with diagramming tools and, if so, which tool(s) they were.

To measure usability, the 10-item *System Usability Scale (SUS)* questionnaire (Brooke, 2013) was used. SUS is an instrument that allows usability practitioners and researchers to measure the subjective usability of products and services. SUS has been utilised in several studies for measuring the perceived usability of modelling languages and their components (Eterovic et al., 2015; Miranda et al., 2018; Nair et al., 2021; Silva et al., 2018; Aboussoror et al., 2013). The 10-item questionnaire can be administered quickly and easily, and it returns scores ranging from 0 to 100. SUS scores can also be translated to adjective ratings, such as ‘worst imaginable’,

‘poor’, ‘OK’, ‘good’, ‘excellent’, ‘best imaginable’ and grade scales ranging from A to F (Bangor et al., 2009). SUS has been shown both to be a reliable and valid instrument that is robust with a small number of participants and to have the distinct advantage of being technology-agnostic, meaning it can be used to evaluate a wide range of hardware and software systems (Brooke, 2013; Brooke, 1996; Tullis and Stetson, 2004; Kortum and Acemyan, 2013).

Next, a general-feedback, open-ended questionnaire was administered to collect the participants’ comments on HORM-DT. The participants were asked the following two questions: i) what they liked about their use of and experience with HORM-DT and ii) what they did not like about it. Participants were free to describe their experiences textually, and there were no follow-up questions from the experimenter’s side.

The main task completion time was measured to document the time needed for participants to reproduce a model for a cybersecurity-related user journey.

Finally, informal observations took place by the experimenter that focused on modelling accuracy; that is, the similarity between the final user-submitted models and the original models provided by the experimenter. The observations were transcribed in a qualitative manner as high level descriptions of similarities and differences.

4.4 Procedure

Due to COVID-19 restrictions, the entire evaluation procedure took place online via the participants’ preferred video-conferencing platform (e.g., Zoom, MS Teams or Skype), with them sharing their screens so that the experimenter could observe their progress.

First, the participants were presented with an introduction to the study, then they provided informed consent and filled out a questionnaire on demographics and their experience with diagramming tools.

The experimenter then presented two tasks. The first was about reproducing a journey diagram model of an online service user journey with a problematic

point/deviation (Figure 6a). It served as the introductory task, and so it was used to introduce participants to the tool and become familiar with it by performing simple actions. For the second task, the participants had to reproduce a swimlane diagram model of a phishing attack against an SME employee (Figure 6b). This was the main task of the evaluation study and, based on pilot testing, its estimated completion time was 25–45 minutes.

The models that had to be reproduced in the two tasks were sent to the participants at the time of the study via the video-conferencing platform as exported images.

There was no time limit for the completion of the tasks, and no external help was allowed for the construction of the diagrams. At the end of each task, the participants had to export their reproduced models in PNG image format and send them to the experimenter via the video-conferencing platform. There was no control or set threshold regarding the modelling accuracy of the tasks (produced vs original) as a requirement for completing the study.

Finally, participants completed the SUS and general feedback questionnaires.

4.5 Statistical Analysis

All data were analysed using the IBM SPSS version 29 software. The significance level was set at $p < 0.05$. Descriptive analysis was used to depict the demographic data of the participants and to analyse the SUS values. Welch's t-test was used to detect differences between the inexperienced and experienced users' SUS scores and main task completion times. The data from the general feedback questions were transcribed and then analysed through open and axial coding, which enabled core concepts, themes and ideas to be identified. Two researchers coded the data independently; the inter-rater reliability was assessed; and any disagreements were identified, discussed and settled.

5 RESULTS

Twenty-nine participants ($N = 29$, mean age: 27.76, SD: 4.48, male/female: 17/12) evaluated HORM-DT. Sixteen participants ($N = 16$, mean age: 26.38, SD: 3.56, male/female: 10/6) had never used diagramming tools before (i.e., *inexperienced* users), and thirteen participants ($N = 13$, mean age: 29.46, SD: 5.03, male/female: 7/6) had experience with diagramming tools such as Draw.io/Diagrams.net, MS Visio, Miro and the diagramming functions of MS Word and MS

PowerPoint (i.e., *experienced* users).

The HORM-DT interface scored a mean SUS value of 80.69 (SD: 12.64). This value provided a usability evaluation of between 'good' and 'excellent', equivalent to a B grade (Brooke, 2013; Brooke, 1996). When the results were analysed and controlled for participants' previous experience with diagramming tools, the following results were identified (Table 1). Experienced users ($N = 13$) awarded a mean SUS value of 82.5 (SD: 14.43), and inexperienced users ($N = 16$) awarded a mean SUS value of 79.22 (SD: 11.24). No statistically significant differences were found between the experienced and inexperienced users' SUS scores, based on Welch's t-test: $t(22.4) = 0.67, p = 0.509$.

Table 1: SUS results for HORM-DT.

Participants	Mean SUS score (SD)
All ($N = 29$)	80.69 (12.64)
– Experienced ($N = 13$)	82.5 (14.43)
– Inexperienced ($N = 16$)	79.22 (11.24)

The mean main task completion time (Table 2) was 35.62 minutes (SD: 17.22); for experienced users ($N = 13$), it was 29.38 minutes (SD: 13.2), and for inexperienced users ($N = 16$), it was 40.69 minutes (SD: 18.79). No statistically significant differences were found between the experienced and inexperienced users' main task completion time, based on the Welch's t-test: $t(26.53) = -1.9, p = 0.069$.

Table 2: Main task completion time results for HORM-DT.

Participants	Mean main-task completion time (SD)
All ($N = 29$)	35.62 min. (17.22)
– Experienced ($N = 13$)	29.38 min. (13.2)
– Inexperienced ($N = 16$)	40.69 min. (18.79)

Table 3 presents the participants' comments collected from the two general feedback questions, together with the frequency of their occurrence. The participants' comments were further characterised as positive (P) and negative (N).

Based on observations regarding modelling accuracy, all participants reproduced the diagrams with very high accuracy, and only some typographical errors and small positioning differences in lines and shapes featured in their produced models.

Table 3: Participants comments as collected from the two general-feedback questions.

	Comment	Count
P	HORM-DT is simple and easy to use.	18
N	It can be challenging to use the arrows to connect objects and form straight lines.	9
P	Icons and graphical objects are clearly designed and categorised.	6
P	Templates are useful and easily accessible.	4
P	HORM-DT is suitable for novice users.	3
P	It is easy to connect objects.	3
N	When inserting text, the default font size is too small.	2
N	HORM-DT does not contain all the libraries of Diagrams.net.	1
N	Some icons are not immediately visible and need to be searched for.	1

6 DISCUSSION

In this work, HORM-DT was designed and developed to be a standalone, open and customised tool for the application of extended CJML within the HORM framework. The tool's UI and functionality were based on the Diagrams.net software and then significantly extended and redesigned to fit the customised needs of the modelling language domain. To that end, a heuristic evaluation of the Diagrams.net UI took place, and new icon libraries and templates were created and new interaction steps regarding model development were introduced, among other changes (Section 3.2). The usability of the tool was central to the study, paving the way for using HORM-DT when examining the effectiveness of the modelling language for raising SME cybersecurity awareness.

Since HORM-DT featured satisfactory and good usability values, based on the SUS score, it can be said that the chosen design and development process contributed to reaching the goal. The usability, simplicity and user-friendliness of the tool were also praised by the participants. The clearly designed icons, graphical objects and useful templates may have contributed to that, based on the participants' comments. On the other hand, the drawing of lines was negatively rated, since Diagrams.net features a very simplistic way of connecting items with lines (by connecting predefined points); however, for new users, this might not have been obvious and required a starting tutorial.

As for the comparison of the perceived usability and main task completion time between experienced and inexperienced users (Tables 1 and 2), there were naturally differences; however, those differences were not found to be statistically significant. Therefore, it may be said that HORM-DT can facilitate use even by users that have no prior experience with diagramming tools and fulfil the goal of enabling modelling by users with diverse technical backgrounds (Section 1).

Finally, in this work, the decision was made to use existing open-source code (i.e., Diagrams.net), instead of starting from the ground up. This happened for the following two reasons: i) Diagrams.net is a widely used tool with a user-friendly UI, and it is used frequently in the modelling-language domain (as mentioned in Section 3.1), and ii) a green coding strategy based on reusing existing code (Verdecchia et al., 2021) was followed. In terms of the latter strategy, this work alone may not have had an enormous environmental impact, but it has helped create a coding attitude towards the environmental goal of reducing software's energy consumption, which can be applied in future projects and contribute to raising awareness about the topic.

6.1 Implications

In this work, the following elements can be generalised and inform the designs of other practitioners and researchers in the field:

- A modelling tool for mapping cybersecurity-related user journeys is openly deployed for use by other practitioners and researchers in their cybersecurity-related use cases. The tool features satisfactory usability and can facilitate modelling by users with diverse technical backgrounds. Moreover, the tool's code is openly distributed for interested parties to further extend and build upon.
- An effective and resource-efficient methodological approach is introduced to measure the perceived usability of modelling tools when the underlying formalism remains the same, albeit with an updated UI. The proposed methodology follows formalism-agnostic logic when the UI of a modelling-language tool is updated so that i) the evaluation results solely address and focus on the updated UI elements and their usability performance, and ii) resources such as time and cost are saved during the evaluation process, since partic-

ipants are not required to become accustomed to the tool's formalism in order to use it for the purposes of the study.

- An extension of the aforementioned methodological approach is also introduced to measure the perceived usability coming from users with diverse attributes (in this case, prior experience with diagramming tools). Therefore, in cases in which a modelling language tool targets a heterogeneous user group, a within-group comparative approach based on the differentiating attribute can benefit the usability measurements and the conclusions that come out of it.

6.2 Limitations

This evaluation study of HORM-DT had the following limitations:

- COVID-19 restrictions affected the evaluation process. Although the tasks were digital and could take place remotely, the qualitative part of the evaluation study might have been carried out in a more effective way with physical attendance, such as through personal interviews. The restrictions also affected the recruitment process, leading to convenience sampling and contributing to the next point.
- Since the majority of the study participants were students from the University of Oslo (i.e., convenience sampling), a participant sample of a young age (mean age: 27.76, SD: 4.48) was recruited. The study participants' technical background and prior experience with diagramming tools may have been affected by their young age.
- The participants, especially those without prior experience with diagramming tools, may have needed detailed guidance to become familiar with drawing lines when using HORM-DT. Nevertheless, the logic behind drawing lines and connecting elements became clear after a while, but a more detailed starting tutorial could alleviate the few negative experiences on that matter, as documented in Table 3.

7 CONCLUSION

In this work, HORM-DT was introduced as a tool for modelling cybersecurity-related journeys to help SMEs to raise cybersecurity awareness and take the first step towards defining or updating their cybersecurity practices. The tool was examined in terms of

the usability its UI offers to users, producing satisfactory and promising results. Apart from the actual tool, which has been openly deployed online and its code is freely accessible, the work also introduced a cost-effective methodological approach for evaluating the usability of modelling tools that have updated UIs but still feature the same formalism. In the future, further work will be conducted on i) developing a starting tutorial (e.g., an introductory video) on how simple HORM-DT diagrams can be made, with an emphasis on drawing lines and connecting objects; ii) exploring the effectiveness of the overall HORM modelling language, as facilitated by HORM-DT, for raising SME cybersecurity awareness and involving various target groups, such as cybersecurity experts and regular, non-technical employees; and iii) developing a text editor as an extension of the tool that would enable users to textually describe their models, which would be automatically translated to diagrams.

ACKNOWLEDGEMENTS

We would like to thank the IVAPP 2023 reviewers for their constructive feedback. This research is funded by the European Commission through the CyberKit4SME project (www.cyberkit4sme.eu) under Grant Agreement 883188. CyberKit4SME will provide cybersecurity tools that help SMEs become aware of, analyse, and manage cybersecurity and data protection risks.

REFERENCES

- Aboussoror, E. A., Ober, I., and Ober, I. (2013). Significantly increasing the usability of model analysis tools through visual feedback. In *International SDL Forum*, pages 107–123. Springer.
- Agárdi, A. (2022). Relontouml model of the archaeological findings. *Production Systems and Information Engineering*, 10(1):64–71.
- Arctic Wolf (2017). The state of mid-market cybersecurity: Findings and implications. https://2p167arhj4lo70dn1q26fm1c-wpengine.netdna-ssl.com/wp-content/uploads/AW_Brief_Midmarket_Cybersecurity_Survey.pdf (Accessed 17 Nov 2022).
- Bangor, A., Kortum, P., and Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123.
- Bellamy, R. K., Erickson, T., Fuller, B., Kellogg, W. A., Rosenbaum, R., Thomas, J. C., and Wolf, T. V. (2007). Seeing is believing: Designing visualizations for managing risk and compliance. *IBM Systems Journal*, 46(2):205–218.

- Benz, M. and Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, 63:531–540.
- Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., and Surrige, M. (2021). Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *VISIGRAPP (3: IVAPP)*, pages 266–274.
- Brooke, J. (1996). SUS - A quick and dirty usability scale. In Jordan, P., Thomas, B., Weerdmeester, B., and McClelland, I., editors, *Usability Evaluation in Industry*, pages 189–194. Taylor & Francis.
- Brooke, J. (2013). SUS: A Retrospective. *Journal of Usability Studies*, 8(2):29–40.
- Chávez-Feria, S., García-Castro, R., and Poveda-Villalón, M. (2021). Converting UML-based ontology conceptualizations to OWL with Chowlk. In *European Semantic Web Conference*, pages 44–48. Springer.
- Chávez-Feria, S., García-Castro, R., and Poveda-Villalón, M. (2022). Chowlk: from UML-based ontology conceptualizations to OWL. In *European Semantic Web Conference*, pages 338–352. Springer.
- Dimitrakos, T., Ritchie, B., Raptis, D., and Stølen, K. (2002). Model based security risk analysis for web applications: the CORAS approach. In *EuroWeb 2002 Conference*, pages 1–13.
- Eterovic, T., Kaljic, E., Donko, D., Salihbegovic, A., and Ribic, S. (2015). An Internet of Things visual domain specific modeling language based on UML. In *2015 XXV International Conference on Information, Communication and Automation Technologies (ICAT)*, pages 1–5. IEEE.
- Fair, N., Phillips, S., Erdogan, G., and Tverdal, S. (2022). Information security & risk management: trustworthiness and human interaction. In *Tutorial proceedings of the 16th International Conference on Research Challenges in Information Science*, pages 1–48. RCIS. <https://www.rcis-conf.com/rcis2022/files/T1-NicholasFairEtAl.pdf>.
- Halvorsrud, R., Boletsis, C., and Garcia-Ceja, E. (2021). Designing a modeling language for customer journeys: Lessons learned from user involvement. In *2021 ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pages 239–249. IEEE.
- Halvorsrud, R., Haugstveit, I. M., and Pultier, A. (2016a). Evaluation of a modelling language for customer journeys. In *2016 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 40–48. IEEE.
- Halvorsrud, R., Kvale, K., and Følstad, A. (2016b). Improving service quality through customer journey analysis. *Journal of Service Theory and Practice*, 24(6):840–867.
- Halvorsrud, R., Lee, E., Haugstveit, I. M., and Følstad, A. (2014). Components of a visual language for service design. In *ServDes. 2014 Service Future, Proceedings of the fourth Service Design and Service Innovation Conference, Lancaster University, United Kingdom, 9-11 April 2014*.
- Haugstveit, I. M., Halvorsrud, R., and Karahasanovic, A. (2016). Supporting redesign of C2C services through customer journey mapping. In *Service Design Geographies. Proceedings of the ServDes. 2016 Conference*, number 125, pages 215–227. Linköping University Electronic Press.
- Jaimez-González, C. and Martínez-Samora, J. (2020). DiagramMER: A Web Application to Support the Teaching-Learning Process of Database Courses Through the Creation of ER Diagrams. *International Journal of Emerging Technologies in Learning (iJET)*, 15(19):4–21.
- JGraph (2022). Features of diagrams.net and draw.io. <https://diagrams.net/features> (Accessed 17 Nov 2022).
- Khan, M. I., Tanwar, S., and Rana, A. (2020). The Need for Information Security Management for SMEs. In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pages 328–332. IEEE.
- Kortum, P. and Acemyan, C. Z. (2013). How low can you go? Is the System Usability Scale range restricted? *Journal of Usability Studies*, 9(1):14–24.
- Kullman, K., Buchanan, L., Komlodi, A., and Engel, D. (2020). Mental model mapping method for cybersecurity. In *International Conference on Human-Computer Interaction*, pages 458–470. Springer.
- Lund, M. S., Solhaug, B., and Stølen, K. (2011). Risk analysis of changing and evolving systems using CORAS. In *International School on Foundations of Security Analysis and Design*, pages 231–274. Springer.
- Meshkat, L., Miller, R. L., Hillsgrove, C., and King, J. (2020). Behavior modeling for cybersecurity. In *2020 Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–7. IEEE.
- Meszaros, J. and Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *computers & security*, 65:300–313.
- Miranda, T., Challenger, M., Tezel, B. T., Alaca, O. F., Barišić, A., Amaral, V., Goulão, M., and Kardas, G. (2018). Improving the usability of a mas dsml. In *International workshop on engineering multi-agent systems*, pages 55–75. Springer.
- Nair, A., Ning, X., and Hill, J. H. (2021). Using recommender systems to improve proactive modeling. *Software and Systems Modeling*, 20(4):1159–1181.
- Nielsen, J. (2020). 10 Usability Heuristics for User Interface Design. <https://www.nngroup.com/articles/ten-usability-heuristics/> (Accessed 17 Nov 2022).
- Nurse, J. R., Creese, S., Goldsmith, M., and Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 60–68. IEEE.
- Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, 49(8):92–97.
- Ponsard, C. and Grandclaoudon, J. (2019). Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs. In *International Conference*

- on *Information Systems Security and Privacy*, pages 335–357. Springer.
- Raptis, D., Dimitrakos, T., Gran, B. A., and Stølen, K. (2002). The CORAS approach for model-based risk management applied to e-commerce domain. In *Advanced Communications and Multimedia Security*, pages 169–181. Springer.
- Rauer, M. (2019). Draw.io diagramming in Confluence is currently the most successful app in the Atlassian Marketplace. <https://blog.seibert-media.com/2019/04/18/draw-io-diagramming-in-confluence-is-currently-the-most-successful-app-in-the-atlassian-marketplace/> (Accessed 17 Nov 2022).
- Shojaifar, A. (2019). SMEs Confidentiality Issues and Adoption of Good Cybersecurity Practices. In *IFIP Summer School on Privacy and Identity Management*, pages 1–8.
- Silva, J., Barišic, A., Amaral, V., Goulão, M., Tezel, B. T., Alaca, O. F., Challenger, M., and Kardas, G. (2018). Comparing the usability of two multi-agents systems DSLs: Sea_ml++ and DSML4MAS study design. In *3rd International Workshop on Human Factors in Modeling*, volume 2245, pages 770–777.
- Skubisz, C., Reimer, T., and Hoffrage, U. (2009). Communicating quantitative risk information. *Annals of the International Communication Association*, 33(1):177–211.
- Slovic, P. (1999). Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield. *Risk analysis*, 19(4):689–701.
- Stickdorn, M., Hormess, M. E., Lawrence, A., and Schneider, J. (2018). *This is service design doing: applying service design thinking in the real world.* O'Reilly Media, Inc.
- Stølen, K. (2001). CORAS – A Framework for Risk Analysis of Security Critical Systems. In *supplement of the 2001 International Conference on Dependable Systems and Networks, pages D4-D11*.
- Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S.-H., Lund, M. S., Stamatou, Y., and Aagedal, J. (2002). Model-based risk assessment – the CORAS approach. In *iTrust Workshop*.
- Surridge, M., Meacham, K., Papay, J., Phillips, S. C., Pickering, J. B., Shafiee, A., and Wilkinson, T. (2019). Modelling compliance threats and security analysis of cross border health data exchange. In *International Conference on Model and Data Engineering*, pages 180–189. Springer.
- Symantec (2019). Symantec 2019 internet security threat report. <https://docs.broadcom.com/doc/istr-24-2019-en> (Accessed 17 Nov 2022).
- The National Center for the Middle Market (2016). Cybersecurity and the middle market: The importance of cybersecurity and how middle market companies manage cyber risks. https://www.middlemarketcenter.org/Media/Documents/the-importance-of-cybersecurity-and-how-middle-market-companeis-manage-cyber-risks_NCMM.Cybersecurity_Report_FINAL.pdf (Accessed 17 Nov 2022).
- Tullis, T. S. and Stetson, J. N. (2004). A comparison of questionnaires for assessing website usability. In *Proceedings of the Usability Professional Association Conference*, pages 1–12. Usability Professional Association.
- Vakaliuk, T. A., Korotun, O. V., and Semerikov, S. O. (2021). The selection of cloud services for ER-diagrams construction in IT specialists databases teaching. In *CTE Workshop Proceedings*, volume 8, pages 384–397.
- Verdecchia, R., Lago, P., Ebert, C., and De Vries, C. (2021). Green IT and green software. *IEEE Software*, 38(6):7–15.
- Von Der Assen, J., Franco, M. F., Killer, C., Scheid, E. J., and Stiller, B. (2022). CoReTM: An Approach Enabling Cross-Functional Collaborative Threat Modeling. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 189–196. IEEE.
- Vraalsen, F., Lund, M. S., Mahler, T., Parent, X., and Stølen, K. (2005). Specifying legal risk scenarios using the CORAS threat modelling language. In *International Conference on Trust Management*, pages 45–60. Springer.