

Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment

Costas Boletsis¹^a, Ragnhild Halvorsrud¹^b, J. Brian Pickering²^c, Stephen Phillips²^d
and Mike SurrIDGE²^e

¹SINTEF Digital, Oslo, Norway

²IT Innovation Centre, University of Southampton, Southampton, U.K.

Keywords: Cybersecurity, Modelling, Socio-technical Risk Assessment, User Journey, Visualisation.

Abstract: Small and medium-sized enterprises (SMEs) rarely conduct a thorough cyber-risk assessment and they may face various internal issues when attempting to set up cyber-risk strategies. In this work, we apply a user journey approach to model human behaviour and visually map SMEs' practices and threats, along with a visualisation of the socio-technical actor network, targeted specifically at the risks highlighted in the user journey. By using a combination of cybersecurity-related visualisations, our goals are: i) to raise awareness about cybersecurity, and ii) to improve communication among IT personnel, security experts, and non-technical personnel. To achieve these goals, we combine two modelling languages: Customer Journey Modelling Language (CJML) is a visual language for modelling and visualisation of work processes in terms of user journeys. System Security Modeller (SSM) is an asset-based risk-analysis tool for socio-technical systems. By demonstrating the languages' supplementary nature through a threat scenario and considering related theories, we believe that there is a sound basis to warrant further validation of CJML and SSM together to raise awareness and handle cyber threats in SMEs.


1 INTRODUCTION


Today, small and medium-sized enterprises (SMEs) can be considered as the new big target for cyberattacks, being among the least mature and most vulnerable in terms of their cybersecurity risk and resilience (Vakakis et al., 2019; Benz and Chatterjee, 2020; Ponsard and Grandclaudon, 2019; Paulsen, 2016). SMEs rarely conduct a thorough cyber-risk assessment and they may face various internal issues 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. As a result, more than half of the existing SME companies lack either an up-to-date cyber-risk strategy or any defined cyber-risk strategy at all (Benz and Chatterjee, 2020;


Paulsen, 2016; The National Center for the Middle Market, 2016). The most challenging tasks for cybersecurity risk management in SMEs include which initial actions should they implement in order to improve their security posture and how to address the human element (i.e., errors made by employees). The latter (the human element) is sometimes referred to as the biggest internal threat faced by SMEs (Arctic Wolf, 2017; Meshkat et al., 2020; Symantec, 2019).


Mapping the SMEs current practices and the potential threats they may face has been suggested as a useful first step in cybersecurity risk management (Benz and Chatterjee, 2020; Paulsen, 2016; Meszaros and Buchalcevova, 2017). This mapping should i) lead to the modelling of human behaviour (i.e., of employees) in cybersecurity-related scenarios and ii) be presented in a comprehensible way (Paulsen, 2016; Kullman et al., 2020; Bellamy et al., 2007).


In this work-in-progress paper, we apply a user-journey approach to model human behaviour and visually map SMEs' practices and threats, along with a visualisation of the socio-technical actor network, targeted specifically at the risks highlighted in the user

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

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

^c <https://orcid.org/0000-0002-6815-2938>

^d <https://orcid.org/0000-0002-7901-0839>

^e <https://orcid.org/0000-0003-1485-7024>

journey. By using a combination of cybersecurity-related visualisations, our goals are: i) to raise awareness about cybersecurity and to potentially reach out to a bigger pool of SME employees, and ii) to improve communication among IT personnel, security experts, and non-technical personnel. More specifically, we combine two modelling languages that supplement each other that supplement each other: Customer Journey Modelling Language (CJML) acts as an upper layer of mapping and visualising cyber threats for clear communication of the problematic behaviours and threatening issues to SMEs' employees, independently of their level of technical expertise. System Security Modeller (SSM) is used at a lower/technical level for mapping cyber threats and mitigating risks and is targeted at IT and security experts.

2 RELATED WORK

Risk communication in the cybersecurity context considers how to best communicate security-risk information to users of a system or process in order to facilitate understanding and promote informed judgement. The risk message itself presents a significant challenge for communication (Nurse et al., 2011). Once a risk message has been investigated and the appropriate information selected for communication, the next crucial question is how should it be presented (Nurse et al., 2011). Three broad formats of presentation have been suggested (Nurse et al., 2011): i) numeric, i.e., using percentages, frequencies and probabilities, ii) verbal, i.e., which applies terms such as "unlikely", "possible", and "definite", and iii) visual, i.e., utilising graphics, graphs, charts, and risk ladders (Nurse et al., 2011; Lipkus and Hollands, 1999; Lipkus, 2007).

Visual mechanisms have become popular formats for communicating risks. The advantage of visuals lies in their ability to attract and engage people's attention, to assist in visualising and portraying part-to-whole relationships, and to capture and summarise large amounts of data and several processes, thus allowing for easier identification of patterns (Nurse et al., 2011) and appreciating relevance (Pickering et al., 2019).

For cybersecurity assessments, simply supplying accurate risk information is not enough to ensure that individuals will be able to process, comprehend, and act on the risk message (Nurse et al., 2011; Slovic, 1999; Skubisz et al., 2009). In providing an intuitive and easily accessible message, visualisations can offer an effective mechanism for communicating cyber risks during cybersecurity assessments. Especially, if

we place SMEs as the risk message receivers in these assessments, then a compelling research field develops. In that field, there are works - yet limited in number - evaluating SMEs' cybersecurity practices, utilising visual elements. Such work is mostly focused on raising awareness among SMEs regarding their cybersecurity maturity level, identifying cybersecurity gaps, and urging them to update their existing or develop new cybersecurity strategies.

Benz and Chatterjee (2020) proposed an SME cybersecurity evaluation tool (CET). The tool consists of a 35-question online survey to be completed by IT leaders to self-rate their maturity within the five NIST¹ Cybersecurity Framework categories: identify, protect, detect, respond, and recover. Survey respondents, i.e., SME IT leaders, get a report card and a recommendation report after completing the survey. The report card presents the survey scores and the cybersecurity gaps on the aforementioned five categories. The recommendation report provides actionable recommendations for each potential gap. Both report cards and recommendation reports are visualised as, mostly, text-based flyers that are handed out to the IT leaders.

Ponsard and Grandclaoudon (2019) followed a gamified approach for raising awareness around SMEs' level of cybersecurity and resilience. SME employees had to answer a cybersecurity quiz composed of a set of questions covering situations like managing passwords, performing backups, explaining concepts like electronic signature among other things. Then, a self-assessment questionnaire was administered, based on the 20 controls of the Center for Internet Security² in order to urge participants to engage with a cybersecurity improvement process.

Shojaifar (2019) presented CYSEC, a DIY cybersecurity assessment method for SMEs. CYSEC automates elements of a counselling dialogue between a security expert and employees in the SME to counter cyber threats. CYSEC coaches SMEs to improve their cybersecurity awareness and capabilities through three key features: i) a self-assessment questionnaire for capturing the state of various security focus areas, ii) training and awareness content embedded in the questionnaire to demonstrate countermeasures against security threats, and iii) recommendations from cybersecurity experts, based on users' responses to the questionnaires, regarding the prevention of cybersecurity compromises.

¹National Institute of Standards and Technology

²<https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/>

2.1 Initial Evaluation

The works reviewed above rely almost exclusively on a top-down approach. By that, we mean they focus on the static representation of an infrastructure, with little reference to human actors, their behaviours or their experiences. Such approaches start with a presentation of generic cybersecurity practices before moving immediately on to specific practices, threats and recommendations aimed at an individual SME. These approaches typically define three main stages in attempting to communicate the need for an improved or completely new cybersecurity strategy to the SME:

1. Mapping existing cybersecurity practices;
2. Identifying potential threats to the business; and
3. Suggesting solutions to mitigate those potential threats.

The first stage usually involves a structured survey of the SME's current processes. The second and third stages include consultations led either by cybersecurity experts directly or by applying cybersecurity frameworks and theory to the output of the first stage. These three stages are informed either by a cross-section of employees at the SME or by IT professionals specifically tasked with cybersecurity implementation and strategy. Such approaches overlook the influence of human actors within a socio-technical system, and how specialist information pertaining to cybersecurity is presented to non-cybersecurity experts. Yet as highlighted in the WannaCry attack (Martin et al., 2018), human responses to a cybersecurity incident significantly affected its impact both directly (what those involved actually do) and indirectly (how ongoing trust relations are affected).

Introducing human behaviours raise two major issues. First, it is essential to appreciate any context dependencies of human actor behaviours (Olli et al., 2001). For example, overall compliance with organisational policies may fail to take account of the different processes undertaken, any individual user reliance on personal assessment, and the interactions between the two (Blythe, 2013)³. Secondly, even tools which are based on an appropriate visualisation (Bellamy et al., 2007) may not take account of adopter understanding and responses (Pickering et al., 2019, 2020).

With regard to the way the information from the three stages outlined above are presented, appropriate visualisations of information produced does not seem to be a high priority. Existing research approaches regarding mapping SMEs' cybersecurity practices, threats and providing recommendations focus on very

³See also work by Acquisti et al. (2015) on privacy attitudes.

limited methods of presentation. Naturally, there are visual elements, e.g., report cards and recommendation reports (Benz and Chatterjee, 2020) and quiz interfaces (Ponsard and Grandclaudon, 2019). However, there is no holistic visualisation approach that could facilitate information distribution between employees of different levels of expertise. What is more, there is no attempt to encourage a complete understanding of the complexity of cybersecurity for the specific target users beyond simple demonstrations for their particular industry or domain. Without differentiation amongst users, their expectations and their working environment, long-term acceptance of cybersecurity tools is unlikely (Rogers, 2010). Further, contextualising human agent experience within familiar contexts is an essential first step in developing stakeholder understanding (Martin et al., 2018; Pickering et al., 2019, 2020).

Given what we perceive to be a gap in previous cybersecurity modelling approaches, specifically with respect to human actors and human users of cybersecurity tooling, we present here two complementary methodologies in respect of providing ecologically valid and meaningful representations of activities (via customer journey modelling, Section 3) and overall infrastructure (using a secure system modeller, Section 4). We then provide a conceptual evaluation based on a representative use case (Section 5). Finally, a theoretical explanation for why these approaches offer significant benefit in raising SME awareness to cybersecurity risks is provided, as well as the plans for future work (Section 6).

3 A USER JOURNEY PERSPECTIVE

Since each SME process and practice essentially represent a pathway through a sequence of events, their modelling and visualisation could be covered by user journey modelling languages. To that end, we extend the validated Customer Journey Modelling Language (CJML) (Haugstveit et al., 2016) to fit our cybersecurity-related purposes. CJML is a visual language for modelling and visualising service and work processes in terms of customer or user journeys. Being centred around humans and human activities, CJML appeals to a broad user group through its simple and intuitive form (Halvorsrud et al., 2016a). CJML is well suited for detailed modelling of processes that extends over time, involving two or more actors who communicate through various communication channels. With its formalised terminology and notation, CJML serves as a unifying language to

ease cross-departmental communication and to document work processes in a systematic way (Halvorsrud et al., 2016b). Its formalised language and notation is particularly suited to technology-based services (Haugstveit et al., 2016).

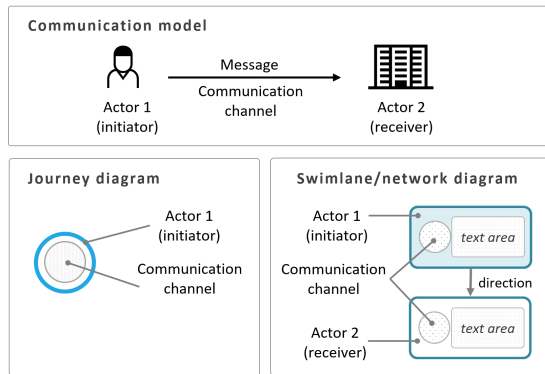


Figure 1: The visual representation of a touchpoint in the case of a journey diagram (left) and a swimlane diagram (right).

The basic units of CJML are the observable touchpoints that can take the form of a communication event or a non-communicative activity or action. A user journey is modelled as a sequence of touchpoints involved for a user to achieve a specific goal. CJML supports two states of a user journey: i) the hypothetical, planned state – as it is intended to unfold in time; and ii) the actual, real journey – as it is experienced in a real context for an individual user. The actual journey may deviate from the planned journey, and results in an experience which is subjective, context dependent, and may change over time (Haugstveit et al., 2016; Halvorsrud et al., 2016a).

In CJML, communication is defined through the Shannon-Weaver model of linear communication (Shannon and Weaver, 1963), where a sender transmits a message to a receiver through a communication channel. There are two types of diagrams available in CJML, serving different purposes. The simple journey diagram is suitable for journeys with few actors and emphasises any deviation from the planned journey. The swimlane or network diagram journeys is useful for journeys involving several actors, and thereby identifies both the initiator and recipient of a touchpoint (Halvorsrud et al., 2016b). Figure 1 shows the relationship between the communication attributes and the touchpoint’s visual representation for the two diagram types.

In this context, CJML is used to document cybersecurity-related user journeys and it features certain adjustments so that the attributes of the extended modelling language cover the cybersecu-

urity domain. More specifically, the users are the SMEs’ employees and external users that make use of the SMEs’ infrastructure under B2B (business-to-business) offerings, and the “deviations” are the cyber threats.

4 A HUMAN-MACHINE NETWORK APPROACH

The System Security Modeller (SSM) is an asset-based risk-analysis tool for socio-technical systems, providing an information-security perspective on the interactions between assets across the whole system. Assets may be people, technology or environments.

The SSM automates much of the risk assessment procedures described in ISO 27005 and thereby supports ISO 27001 compliance. With such automation, the risk assessment becomes systematic and reproducible allowing a security analyst to work more efficiently (Surrige et al., 2019). Using the SSM involves:

1. Draw a model of the system, including relevant assets (networks, hosts, processes, data, people, places) and their relationships, such as which process uses what data (Fig.2).
2. Identify the primary assets for the business (generally data and processes) and indicate the impact on the business that failures in those assets (such as loss of confidentiality) would cause. The SSM then finds the threats to the system automatically using the built-in domain knowledge base and through its understanding of attack-paths and threat cascades.
3. Specify what security control measures are already in place (such as passwords, firewalls, etc). The SSM then computes the risk of every threat to the system automatically. This is challenging by hand and would be done by a security analyst. It involves the use of the specified impacts, the interconnectedness of the assets (to see how failures in the secondary assets affect the primary assets) and

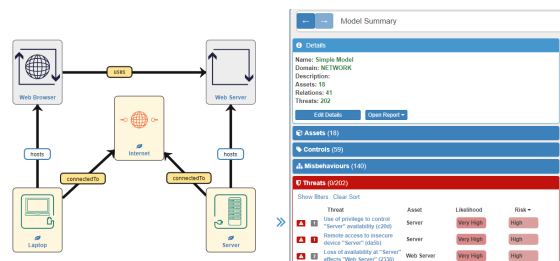


Figure 2: An example model and the user interface of SSM.

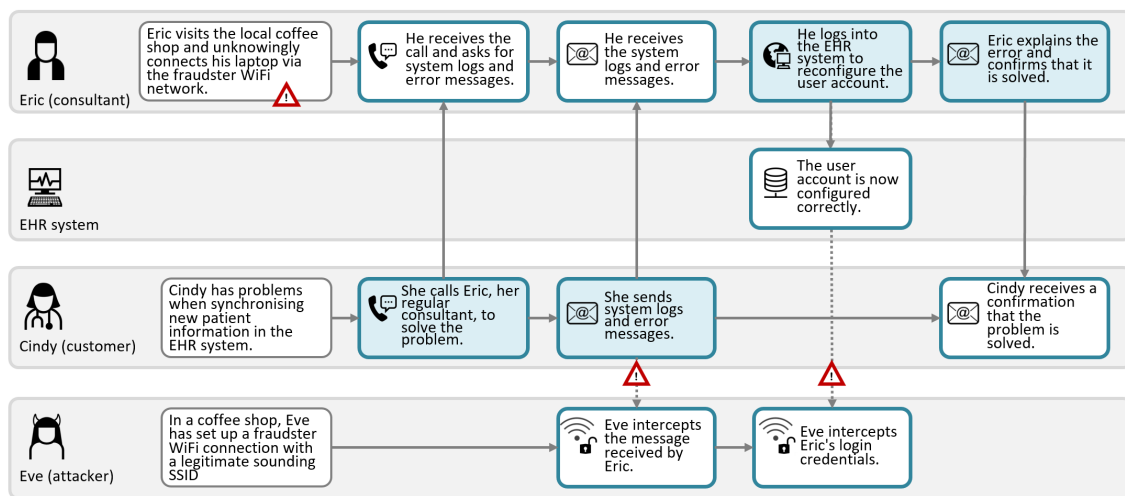


Figure 3: The application of CJML in the threat scenario.

an understanding of how the controls that are in place affect the likelihood of each threat.

4. Examine the high-risk threats to the system, using the SSM to understand the root causes and where controls to reduce the risk can best be placed. Add additional appropriate security controls are suggested by the SSM and the risk is recomputed, repeating this process until the residual risk is acceptable for the business (Surrige et al., 2019).

The SSM models draw on the knowledge often held by multiple people in an organisation and just the construction of the models themselves has value in bringing the information into one place and documenting it. The fact that this "documentation" can then be reasoned over by a computer and combined with an information-security knowledge base makes the tool a powerful one.

5 CASE STUDY

To better demonstrate the mapping and visualisation elements of CJML and SSM, as well as their interconnectivity, an application of the two modelling languages in a mock threat scenario, inspired by the preliminary and formal interviews we had with SMEs' representatives, is presented as a case study. The scenario follows:

Eric works for HealthRec, a company specialised in software for patient administrative systems and electronic health records (EHR) for municipal doctors' offices. Eric works as a customer consultant, and his main tasks are answering customer inquiries and developing training material.

After the COVID-19 outbreak, Eric works mostly from home. From time to time, he brings his laptop down to the local coffee shop to have a change in working environment. As a regular guest, Eric's laptop automatically connects to the shop's WiFi network.

While working on the new user manuals he receives a call from Cindy, a general practitioner in one of their customer sites. She cannot synchronise patient journals that contain new lab results, that are imported from another system. Eric asks her to send the system log and error messages and promises to prioritise her problem. Five minutes later he receives the e-mail from Cindy. He immediately understands the reason for the error messages, which have to do with Cindy not being assigned the correct editing privileges. He quickly upgrades her user account to the correct level and confirms through an e-mail that the problem is fixed.

In the same coffee shop, Eve, a cybercriminal guest has set up a WiFi access point duplicating the coffee shop's SSID and password. When Eric arrived in the coffee shop, he unknowingly used the cybercriminal's WiFi access point. Eve can now monitor Eric's online activity, intercept his login credentials to the EHR system, and other data being transmitted and received over the network. The consequences may be severe, now that Eve has Eric's login credentials, as a system administrator in platforms used in municipal doctors' offices.

5.1 Applying the CJML

The CJML visualisation of the threat scenario is presented in Fig. 3. A network journey diagram is used since the user scenario involves several actors. The

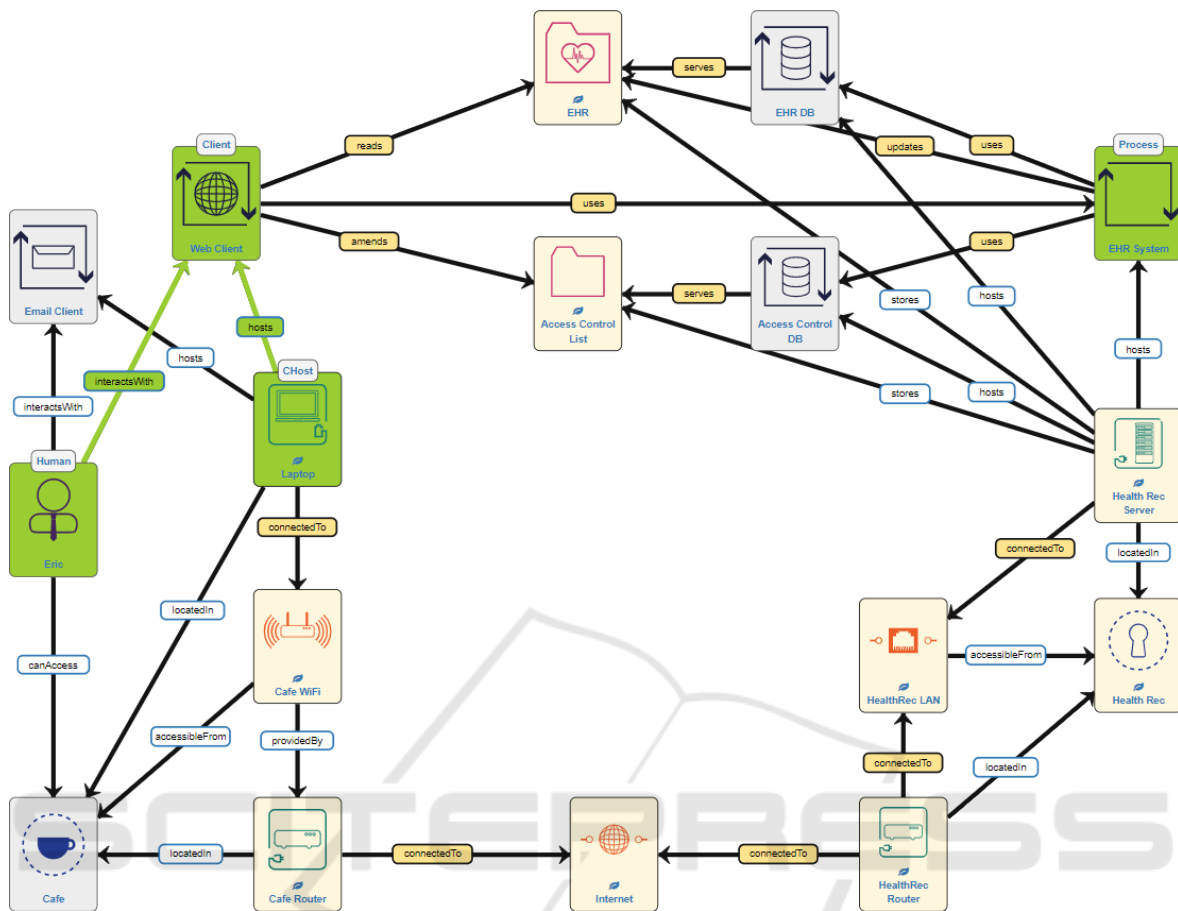


Figure 4: The application of SSM in the threat scenario with a snooped communication threat highlighted.

actors’ touchpoints are organised in horizontal paths in a chronological order from left to right. The CJML model uses action elements to explain the context of each actor, and in Eric’s case it reveals the fatal Internet connection through the fake WiFi access point. A warning sign is introduced throughout to emphasize cybersecurity threats and potential consequences.

The first communication point in the model is Cindy’s telephone call to Eric when having problems with synchronising patient journals. Immediately after the call she initiates a second touchpoint by sending an e-mail. At this point, a new warning sign appears in the diagram as the attacker Eve intercepts the e-mail message. Next, a second data breach takes place as Eve accesses Eric’s login credentials to the EHR system. Still unaware about the man-in-the-middle attack, Eric sends an e-mail to Cindy in the last step of the CJML model.

5.2 Applying the SSM

Using the SSM we have modelled the same scenario (Fig. 4). Such a model would generally require input from various people to construct (network administrator, software and data specialists) and when completed helps communicate the system as well as the threats.

The SSM is used to model the “sunny day” scenario (where the system is operating normally) and so “Eve” and her fake WiFi access point are not explicitly modelled but attackers of all kinds are automatically considered. To simplify the model slightly, the data sent to and from Eric’s email client has also been omitted.

The primary assets in this model are the Access Control List and EHR datasets. The impact of loss of confidentiality on these datasets has been set to “medium” and “high” respectively. A reasonable set of baseline controls were added, such as firewalls, passwords, anti-malware, secure configuration, secure BIOS, software patching, etc.

The initial model analysis and risk calculation by the SSM finds many threats to the system and calculates that the highest-risk threat consequence is the loss of confidentiality of the EHR dataset. When the causes of the loss of confidentiality are queried, the SSM identifies the threat of the “Cafe WiFi” network being spoofed as the primary root cause and also identifies the threats of snooped communication (in general) between the “Web Client” and the “EHR System” as well as the specific case of the snooped password between the two systems.

The SSM user makes use of various displays describing threats to the system and their consequences, and is also shown options, where available, to add security measures to reduce risk.

A couple of security measures are proposed by the tool to ensure that the laptop connects to the genuine Cafe Wifi but, in this situation where the password is public and systems administrator help is not available, they are not appropriate.

Examining the snooped password threat reveals three proposed security controls, all different ways to provide an additional authentication factor. i) The addition of a one-time key such as through an authenticator app on a phone or a separate physical device; ii) an out-of-band key such as that sent via a text message; or iii) a continuous authentication system that monitors the characteristics of the usage of Eric’s laptop. Any of these controls would render the capture of the password useless but the use of an additional factor does not prevent the data accessed by Eric once authenticated being snooped.

To prevent the snooping of data diverted over the spoofed WiFi, the SSM recommends encrypting the communication between the “Web Client” and the “EHR System” (these assets are highlighted in Fig. 4). This not only makes snooping the password impossible but prevents the snooping of other data such as the updated Access Control List. Just encrypting the communication without also adding a second authentication factor still leaves the system open to credential-stuffing attacks: both controls should be used.

Adding these controls and recomputing the risk shows that they do indeed bring the risk of loss of confidentiality of the EHR dataset down to an acceptable value. The security controls proposed by the system in this case would be unavoidable if implemented, requiring no user choices. We might question the wisdom of Eric accessing such data from a public space (especially without such controls being in place). The SSM does model the trustworthiness of the users, which in turn links to the decisions taken by the actors in the CJML model.

6 CONCLUSION & FUTURE WORK

In this work, we have introduced a combination of cybersecurity-related visualisations to raise awareness about cybersecurity and to improve communication among security experts and non-technical personnel in SMEs. The human-centred CJML diagram shows all the actual communication points between the actors in the threat scenario. The target group of this diagram is wide, and previous research shows a high adoption among non-technical personnel. The SSM asset-based risk-analysis tool addresses the security risks and the requirements to be assessed in the scenario. Overall, we have demonstrated the two languages’ supplementary nature through a hypothetical threat scenario.

Although we have presented a limited conceptual validation of our modelling approach, there is some theoretical evidence which indicates that the visualisations we are working on will benefit the target users. The Job Characteristics Model (JCM) emphasises the possible effects of certain features of a task, such as its significance and the degree of autonomy it affords those responsible in relation to the psychological effect working the job is likely to promote (Hackman and Oldham, 1976), and more recently the potential to exploit the model to encourage psychological buy-in (Pierce et al., 2009). This in turn encourages a sense of responsibility and increased performance. We maintain that the context-specific and relevant model visualisations that we have presented here optimise the perceived job characteristics to enhance autonomy and encourage intrinsic motivation and psychological ownership of cybersecurity for all actors within the complex socio-technical systems described by the SMEs we interviewed.

Perhaps more importantly is the co-presentation both of risk and threats together with the mitigation strategies. This corresponds well with constructs in the Health Belief Model (HBM) (Carpenter, 2010; Champion and Skinner, 2008). According to this model, originally applied to behavioural change in healthcare and health interventions but also shown to be relevant to other areas (Lindsay and Strathman, 1997) predicts that awareness of risk (which both CJML and SSM foreground) and its severity or negative outcomes (the impacts of SSM) encourage active engagement. Coupled with that, individuals develop a feeling of self-efficacy which gives them the belief, just as the intrinsic motivation and psychological ownership encouraged with the Job Characteristics Model, that they are capable of dealing with the threat (the mitigation strategies in the SSM tool). Tak-

ing both theories in combination (JCM and HBM), therefore, we believe that there is a sound theoretical basis to warrant further validation of CJML and SSM together to raise awareness of cyber threats and encourage proactive engagement within SMEs to be able to handle those threats, i.e., to encourage desired cybersecurity behaviours.

As future work, we will carry out validation case studies with SMEs in four different business sectors. As a starting point, we will define representative scenarios and environments where the tools should be effective. We will then apply the tools and investigate how they support i) the identification and analysis of risks, ii) communication among security experts and non-technical personnel, and iii) general cybersecurity awareness across organisational units and roles.

ACKNOWLEDGEMENTS

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

- Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.
- 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 09 Aug 2020).
- 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.
- Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. In *Proceedings of CHIItaly 2013 Doctoral Consortium*, volume 1065, pages 92–101. CEUR Workshop Proceedings.
- Carpenter, C. J. (2010). A meta-analysis of the effectiveness of health belief model variables in predicting behavior. *Health communication*, 25(8):661–669.
- Champion, V. L. and Skinner, C. S. (2008). The health belief model. In Glanz, K., Rimer, B. K., and Viswanath, K., editors, *Health behavior and health education: Theory, research, and practice*, pages 45–65. John Wiley & Sons, 4th edition.
- Hackman, R. J. and Oldham, G. (1976). Motivation through the design of work: Test of a theory. *Organizational behavior and human performance*, 16(2):250–279.
- Halvorsrud, R., Haugstveit, I. M., and Pultier, A. (2016a). Evaluation of a modelling language for customer journeys. In *Proceedings of 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.
- 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.
- Kullman, K., Buchanan, L., Komlodi, A., and Engel, D. (2020). Mental model mapping method for cybersecurity. In *Proceedings of the International Conference on Human-Computer Interaction*, volume 12210, pages 458–470. Springer.
- Lindsay, J. J. and Strathman, A. (1997). Predictors of recycling behavior: an application of a modified health belief model 1. *Journal of Applied Social Psychology*, 27(20):1799–1823.
- Lipkus, I. M. (2007). Numeric, verbal, and visual formats of conveying health risks: suggested best practices and future recommendations. *Medical decision making*, 27(5):696–713.
- Lipkus, I. M. and Hollands, J. G. (1999). The visual communication of risk. *JNCI monographs*, 1999(25):149–163.
- Martin, G., Ghafur, S., Kinross, J., Hankin, C., and Darzi, A. (2018). WannaCry - a year on. *BMJ*, 361.
- Meshkat, L., Miller, R. L., Hills Grove, C., and King, J. (2020). Behavior modeling for cybersecurity. In *Proceedings of the 2020 Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–7. IEEE.
- Meszaros, J. and Buchalceva, A. (2017). Introducing ossf: A framework for online service cybersecurity risk management. *Computers & security*, 65:300–313.
- Nurse, J. R., Creese, S., Goldsmith, M., and Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 60–68. IEEE.
- Olli, E., Grendstad, G., and Wollebaek, D. (2001). Correlates of environmental behaviors: Bringing back social context. *Environment and behavior*, 33(2):181–208.
- Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, 49(8):92–97.
- Pickering, B., Bartholomew, R., Janian, M. N., Moreno, B. L., and Surridge, M. (2020). Ask me no questions: Increasing empirical evidence for a qualitative approach to technology acceptance. In *Proceedings*

- of the International Conference on Human-Computer Interaction*, pages 125–136. Springer.
- Pickering, B., Janian, M. N., Moreno, B. L., Micheletti, A., Sanno, A., and Surrudge, M. (2019). Seeing potential is more important than usability: Revisiting technology acceptance. In *Proceedings of the International Conference on Human-Computer Interaction*, pages 238–249. Springer.
- Pierce, J. L., Jussila, I., and Cummings, A. (2009). Psychological ownership within the job design context: Revision of the job characteristics model. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, 30(4):477–496.
- Ponsard, C. and Grandclaoudon, J. (2019). Guidelines and tool support for building a cybersecurity awareness program for SMEs. In *Proceedings of the International Conference on Information Systems Security and Privacy*, pages 335–357. Springer.
- Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.
- Shannon, C. E. and Weaver, W. (1963). *The mathematical theory of communication*. University of Illinois Press.
- Shojaifar, A. (2019). SMEs confidentiality issues and adoption of good cybersecurity practices. In *Proceedings of the IFIP Summer School on Privacy and Identity Management*, pages 1–8.
- 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.
- Surrudge, 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 *Proceedings of the 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 19 Aug 2020).
- 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 09 Aug 2020).
- Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K., and Tzouvaras, D. (2019). Cybersecurity in SMEs: The smart-home/office use case. In *Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–7. IEEE.