Design for Cybersecurity (DfC) Cards: A Creativity-Based Approach to Support Designers' Consideration of Cybersecurity

Vivek Rao[1*], Euiyoung Kim[2], Hyun Jie Jung[3], Kosa Goucher-Lambert[4], Alice M. Agogino[5]
[1,4,5] Department of Mechanical Engineering, University of California, Berkeley, US
[2] Department of Design Organization Strategy, Technical University of Delft, NL
[3] Department of Media Studies, University of California, Berkeley, US
*Corresponding Author Contact Information: vivek.rao@berkeley.edu

As new products exhibit increasing connectivity, cybersecurity will become ever more important to the safety and functionality of these new offerings. Product designers, however, struggle to integrate cybersecurity with other considerations during early-stage design. This paper develops an approach to help designers engage with cybersecurity, articulated as a card-based intervention to support three well-defined modes of engineering design creativity: analysis, generation, and evaluation. Developing cybersecurity support questions for each of those modes across the Research, Analyze, Ideate, Build, and Communicate phases of the human-centered design process, we assemble 15 cards total. A human subjects study using the cards was conducted with 33 students in a design course, validating that novice designers found value in the cards when engaging with a diverse range of design projects. This work adds design creativity to the broad dialogue around cybersecurity education, and forms a foundation for further creativity- and design-process-based interventions in cybersecurity.

Design Computing and Cognition DCC'20. J.S. Gero (ed), pp. 357-376.

Introduction

As new products and services continue to exhibit increasing digital connectivity, cybersecurity will become crucial to their safe and effective function [1]. Consideration of cybersecurity is particularly important in the early stages of design, where designers have an opportunity to establish security across the product or system [2]. Despite the urgency of cybersecurity in connected devices, vulnerabilities remain ubiquitous in connected systems [3]. There are a myriad of reasons for such vulnerabilities. Design teams fail to integrate cybersecurity into their designs in part because of a lack of designers' awareness and understanding of the subject, described in a recent study of medical device security [4].

In the early stages of design, product designers must reconcile and synthesize a range of competing interests and factors in their work [5], [6]. Indeed, balancing such factors, e.g. user needs, resources, and requirements, is an essential aspect of the five phases of the human-centered design process: Research, Analyze, Ideate, Build and Communicate [7], [8]. Cybersecurity is often not considered as one of these factors, and, when considered, is typically not considered as the 'essential design principle' it ought to be [9]. While strides towards integrating cybersecurity practices are increasingly common among software engineering teams [10]–[12], consideration of cybersecurity among early stage conceptual product design teams is less explored. When cybersecurity is engaged, it can often be rendered as a constraint [13], which when positioned as a 'rule-based' design approach, can limit teams' ability to engage creatively, and ultimately, to innovate [14]. Researchers have also suggested that end-users do not engage with cybersecurity due to its intangibility, hampering systems designers' work [15]. We extend this lack of tangibility to designers' awareness of cybersecurity. Taken together, these findings suggest that while considering cybersecurity, design teams' creativity throughout the journey of designing must be promoted rather than unnecessarily constrained. We believe that increased tangibility offers one approach to help resolve this tension. Navigating this tension is an essential challenge to establish simultaneously innovative and secure product functions.

In this work, we propose the Design for Cybersecurity (DfC) cards, which embody an approach grounded in design creativity to help guide designers to integrate pro-cybersecurity behaviors and principles in early-stage human-centered design projects. Our work is driven by the insight that designer creativity is often limited by engaging with a specialized, high-complexity space, like cybersecurity, and rather than propose heuristics to defixate designers' work [16], [17], as has been successful in design ideation

support, we provide prompts to help designers engage creatively with every stage of the human-centered design process. This work addresses three research questions:

1. How can we support designers as they integrate cybersecurity across every phase of the human-centered design process?
2. In what phases of the human-centered design process do designers find utility in cybersecurity support?
3. In what types of design projects do designers find utility in cybersecurity support?

The main contributions of this work are to introduce design creativity to the broad dialogue around cybersecurity education for practitioners and designers, and to present the first study of supporting designers' engagement with cybersecurity across the entire human-centered design process.

Background and Related Work

In this section, we first consider foundational and recent examples of tangible, card-based interventions to support the engineering design process, drawing from literature in the engineering design research and human-computer interaction (HCI) communities. Next, we consider major work in tangible cybersecurity awareness and education, with a focus on examples of interactive and card-based support tools. These examples represent manifestations of various frameworks, and motivate our approach manifested as a card-based system.

Card-based Interventions for Design Support

Card sets are a popular platform for design process support among both industry practitioners, e.g., IDEO's Method Cards, [18]–[21] and academic researchers, e.g. SUTD's IDC Cards [16], [17], [22], [23]. Cards are often chosen for their role as 'transfer vehicles' of theoretical knowledge to the designer [23] and, by virtue of their physical form, their ability to facilitate designers' "making design moves on a conceptual level" [24]. The physical form of cards has also allowed them to be effectively used alongside other traditional design process tools and artifacts, such as prototypes and concept sketches [25]. Woelfel's review explored 18 distinct card-based design support tools [26] and categorized cards into three groups: *general purpose 'repository' cards* to store methods; *customizable cards* to instruct designers at various stages of the process; and *context-specific cards* that help designers

navigate a specific design agenda or context. Our work combines elements of both 'customizable cards' and 'context-specific cards,' and we focus our review there.

Among the category of 'customizable cards,' Lauff recently developed principle cards to help early-stage designers engage with additive manufacturing across the design process, from design-for-manufacturing to business modeling [27]. The cards were structured around a syntactic architecture connecting guideline rationales with underlying design approaches, and were supported by images as stimuli. Lauff's contribution focused on enabling design teams to defixate on ready solutions given the possibilities of additive manufacturing. Yilmaz extracted heuristics from existing products to help support designers during conceptual ideation, articulated them as cards, and demonstrated the cards' ability to produce student designs that were rated as more varied and creative than otherwise [16], [17], [28]. Both Lauff and Yilmaz support designers as they are *ideating*, whether about mechanism design, manufacturing, or strategy.

Among the category of 'context-specific cards,' recent work has used cards to communicate context-specific knowledge to designers. Haesling and Raeblid presented Sustainability Design Cards, which capture key generalizable principles of 'design for longevity,' along with key contextualizing information relating each principle to other aspects of sustainable design [29], [30]. The authors' goal was to help designers consider sustainable design in all phases of the design process. Lucero's PLEX cards drew on anthropology and play research to inspire designers creating experiences exhibiting 'playfulness.' Lucero's user study indicated that designers found PLEX cards more helpful than other design methods, e.g., affinity walls, when ideating about playful products, services, and experiences [31]. Deng's work on the Tango Cards sought to translate decades of research in tangible user interfaces (TUIs) and digital games into a 25 cards describing *design consideration questions* to help designers take advantage of well-defined design principles [23].

Our contribution extends from Deng's work by centering on consideration questions rather than heuristic guides. Furthermore, we follow Haesling, Raebild, and Lucero's models of applying cards to design support in a novel context: cybersecurity. Finally, we build on Lauff and Yilmaz's contributions by ensuring that our cards are grounded in a clear syntactic architecture, but extend beyond the ideation phase to support designers across the entire human-centered design process.

Cybersecurity Education and Awareness Interventions

Engineers and designers' awareness of cybersecurity is a nascent area of research. Kim found that while simple interventions to promote cybersecurity demonstrated early improvements in awareness, sustained awareness across the design process was elusive [32], [33]. Kim's work highlights that despite the promise of tangible cybersecurity awareness interventions, keeping cybersecurity interventions relevant to changing design activities remains challenging. Software engineering researchers have developed security design curricula [10], [11], [34], [35], but these are articulated towards the specific challenge of secure software systems design or user interface features, and are less applicable to challenges faced by product designers in early-stage conceptual design.

Interventions at varying levels of tangibility have been proposed to support end users' and designers' engagement with cybersecurity. Among end-users, Huynh used activity theory to develop a story-based interactive game to train users about how cybersecurity functions in their organization [36]. Nestler's 10-card cybersecurity principle deck describes cybersecurity scenarios end-users may encounter [37]. Jin created a 3D role-playing game challenge to communicate cybersecurity principles to high school students [38], while efforts to use mixed reality to train data center employees on security practices were shown to be promising [39]. Coles-Kemp and various collaborators have proposed a range of interventions, from sociological approaches to empathize with and deconstruct insider threats, to comic-book based methods to articulate personas relevant to information security [40]–[43]. Denning's Ctrl-Alt-Hack boardgame illustrated the value of high-interactivity narrative interventions, and was made commercially available [44], [45]. Specifically engaging designers, Denning's Security Cards helped practitioners brainstorm various cybersecurity threats that their product or service might be exposed to [46]. Merrill's adversarial personas cards [47] helped designers envision adversaries and their motivations to design more secure systems.

Our work builds on this range of tangibilities by establishing our design support tool in the cards format, as per Denning and Merrill. We specifically seek to engage early-stage designers. Extending on Denning and Merrill's work to help designers *identify threats*, thus encouraging their pre-emption through design, we seek to integrate cybersecurity into human-centered design practices that can lead to secure products, services, systems, and experiences across every stage of the design process. As described previously, a key goal of ours is to preserve design creativity while providing designers opportunities to engage with cybersecurity.

Methods

In this section, we present our approach to conceptualizing, articulating, and testing the Design for Cybersecurity cards in a human subjects study. We first review the rationale behind the cards, drawing on design creativity research to inform the selection of each card's questions. Next, we describe the structure and presentation of the card set. Finally, we describe methods to test the cards in a human subjects study with novice designers.

Card Rationale & Development

Inspired by Deng's approach to framing design support as design considerations [23], we articulate our cybersecurity support as a series of questions to support designers across each stage of the human-centered design process. A key goal of our work is to embrace design creativity, which exists across all stages of the human-centered process, not just ideation. We ground our discussion of creativity across the design process in Howard's work to explore patterns between the engineering design community's description of design process with that of the cognitive psychology community's description of creative process. Briefly, Howard first reviewed more than 100 different design and creative processes, and argued that creativity could exist across the design process as a cyclical process of *analysis, generation,* and *evaluation* of information, ideas, and reclarifications [48]. *Analysis* is "the continual interpretation and use of information," with corresponding creative activities of 'framing' and 'problem definition.' *Generation* can be broadly understood as divergent thinking - generating ideas. In contrast, *evaluation* is convergent thinking, selecting and reflecting on ideas. Together, these three dimensions underpin creative processes, which Howard postulates operate cyclically in all engineering design activities. In later work, Howard combines this perspective with Gero's foundational description of the engineering design process as articulating function, behavior, and structure (FBS) [49], [50]. While Howard specifies that particular creativity modes align with specific transformations within Gero's FBS framework, it is our belief that in the context of the human-centered design process [7], [8], Howard's original hypothesis of cyclical creative process across design phases holds.

Table 1. Card content by phase and creativity mode.

Design Phase	Creativity Mode	Design Consideration
Research	Analysis	Whose data and privacy are the most vulnerable in our project?
Research	Generation	How might we make our target interviewees feel comfortable talking about their data and privacy?
Research	Evaluation	Have we identified what vulnerable users are most worried about?
Analyze	Analysis	What methods can we use to identify and surface cybersecurity issues from our research findings?
Analyze	Generation	How might we integrate cybersecurity when articulating our design opportunities?
Analyze	Evaluation	Does our framework successfully identify users' frustrations and painpoints related to cybersecurity?
Ideate	Analysis	What specific cybersecurity-related painpoints does our design solution need to resolve?
Ideate	Generation	How might we prioritize the importance of our identified cybersecurity risks in shaping our design concept?
Ideate	Evaluation	Does our solution strengthen users' awareness of data and privacy risks?
Build	Analysis	What features and functions of our prototype would enhance our users' cybersecurity awareness?
Build	Generation	How might we use this prototype to help us get feedback on users' perception of cybersecurity?
Build	Evaluation	Have we learned about how users perceive our solution's impact on cybersecurity?
Communicate	Analysis	What specific cybersecurity-related issues were resolved by the project?
Communicate	Generation	How might we convince the users of the value of cybersecurity in our project?
Communicate	Evaluation	Does the final deliverable address the key cybersecurity issues or risks that we identified?

Thus, we structured our cards around providing design considerations framed to support designers' engagement with cybersecurity as a creative process with discrete *analysis*, *generation*, and *evaluation* stages. Analysis cybersecurity design considerations asked designers to establish a frame in which they were operating in that particular stage. Generation cybersecurity design considerations asked designers to explore many different possibilities within the key activities of that design phase. Finally, evaluation cybersecurity design considerations asked designers to reflect on the work they had completed in that design phase (Table 1). Mapping these three creativity modes across the five design phases (Research, Analyze, Ideate, Build, and Communicate), we developed fifteen cards. Multiple questions were brainstormed for each card, and the research team converged on questions that most effectively addressed key cybersecurity issues relevant to the design phase. For example, in the research phase, questions were grounded in helping design teams identify vulnerable users, a known issue of urgency in designing for cybersecurity [51].

Cards were sized at 4 x 6 inches and printed on card stock. For each card, a representative image was selected to help designers better understand the context of each question. For example, in the example described earlier, an image of two persons viewed by numerous cameras is used to represent the keyword 'vulnerable' (Fig. 1). All images used are royalty-free. Each design phase was color-coded and numbered in the order of the creativity modes to allow designers to sequence their use of the cards.

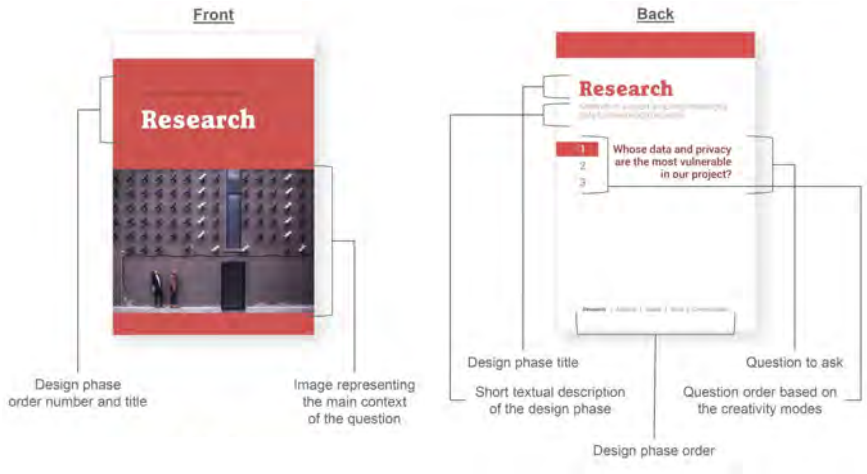


Fig. 1. Example card and overview of card architecture (Download full-size card decks (PDF) - http://bravo.berkeley.edu/wp-content/uploads/2019/08/Design-for-Cybersecurity-DfC.pdf).

Human-Centered Design Participant Study

We tested the cards in a project-based human-centered design engineering course at a major research university in the United States. 33 students of novice designer experience engaged in a semester-long design project centered on mobility, with 14 female and 19 male students. 22 students were international students, and 11 were domestic.

Over the course of six weeks, students formed 3-4 person project teams and worked through the human-centered design process. We classified projects based on Ceschin's framework of innovation levels for projects in sustainability [52] (Table 2). We also apply a simple cybersecurity risk potential assessment to each project, based on a high-medium-low criticality ranking of cybersecurity threats used in practice; the ranking represents a composite of the likelihood and severity of a cybersecurity threat in the particular topic [53]. During the five weeks of class in which students engaged with their projects, one card was distributed per class meeting, sequenced with students' location in the design process. Each week corresponded to a stage of the design process (Fig. 2). Students engaged with three cards per phase, and their distribution was sequenced with the order of activities - within each phase, analysis, generation, and evaluation cards were distributed as students were introduced to the phase, explored the phase, and reviewed their work during the phase, respectively.

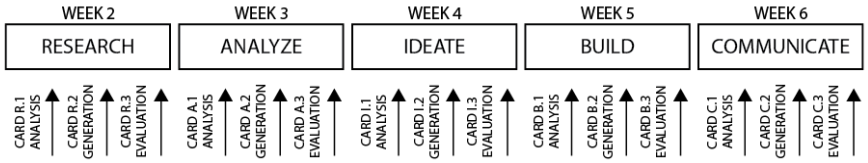


Fig 2. Sequencing of card interventions across the phases of the design process.

To measure designers' perceived utility of the cards in their work, following receipt of the cards, students were asked to answer the question, "How helpful did you find the question on today's card in helping advance your design project?" on a 5-point Likert Scale, with possible values of 'Not helpful at all' (1) to 'Very helpful' (5). Students were asked to complete one survey after receiving each card, for a total of 15 surveys per student. We note that due to a data collection error, responses for card 12, 'Build - Evaluation' were not successful, and have been omitted from results below.

Results

In this section, we present data from our human subjects study on the perceived utility of the cards: (1) overall, (2) by design phase and creativity mode, and (3) by team and project type.

Table 2. Project and cybersecurity risk classification for user study.

Innovation Level	Definition	#	Project Topics	Cybersecurity Risk
Product	improving or developing new **products**.	4	Device to help populations with memory issues navigate their environment	Medium
		6	Personalized wire and electronics organizing	Low
		7	Personalized tableware	Low
		8	Portable, safe, and resilient drinkware	Low
Product-Service System	integrated **combinations of products and services**	5	Tool to digitally capture inspiration	High
		9	Wireless power charging network	High
Spatio-Social	human settlements and the **spatio-social conditions of their communities**, from neighborhoods to cities.	1	Reimagining bus transit planning	High
		2	Digital-physical tools to enhance property safety in public spaces	High
		3	Digital system to ensure nutritional safety for populations with allergies	High
Socio-Technical System	supporting **transitions to new socio-technical systems** (e.g. related to nutrition, transportation, etc.)	N/A		

Overall Perceived Utility of Cards

33 students were surveyed over 14 cards, with 412 data points collected in total. The cards were perceived to have positive usefulness by designers (mean = 3.81, sd = 0.87). 279 responses were positive, scoring a '4' or a '5', indicating designers found the card 'somewhat useful' or 'very useful.' This suggested that designers across the course found the cards helpful in advancing their design work.

To examine the perceived utility of the cards by phase and creativity mode - essentially, examining utility by each card separately - we observe the distributions of perceived utility for each card. The Research-Generation card, card two, was deemed most useful (mean = 4.06, sd = 0.79, n = 33), while the Build-Generation card, card eleven, was deemed least useful (mean = 3.59, sd = 0.95, n = 29). The differences in mean perceived utility across (1) single factors of creativity mode or design phase, (2) two factors of creativity mode and design phase and (3) the fourteen separate cards, was determined to be not statistically significant (Kruskal-Wallis test with factor of creativity mode or design phase, $p > 0.05$; two-way ANOVA with factors of design phase and creativity mode, type 3 sum-of-squares, $p > 0.05$; Kruskal-Wallis test with factor of card, $p > 0.05$). We thus cannot argue that particular design phases, creativity modes, combinations of design phases and creativity modes, or cards were perceived to be more useful than others.

Perceived Utility by Design Team and Project Type

To examine how team influenced perceived utility of cards, we observe team-specific distributions of utility (Fig. 3). Team 7, a product innovation team with four members, found the cards most useful (mean = 4.56, sd = 0.60, n = 54), while team 5, a product-service system team with three members, found the cards least useful (mean = 3.39, sd = 1.07, n = 28). The differences between team means was deemed to be statistically significant (Kruskal-Wallis test comparing response values across teams; $p < 0.05$). A post-hoc Dunn test was conducted to determine the significance of pairwise differences between teams. Among 36 comparisons, 13 differences were deemed significant ($p < 0.05$). Among these comparisons, however, the only team that was consistently significantly different from all other teams was team 7, accounting for 8 of the significant comparisons. Thus, we can conclude that team 7, pursuing a product innovation project, found cards more useful than other teams. We also note that teams 1, 2, and 3, differed significantly ($p < 0.05$) from one another. All of these teams were pursuing spatio-social projects.

To examine how project type influenced perceived utility of cards, we observe type-specific distributions of utility. Product innovation projects found the cards most useful (mean = 3.91, sd = 0.81, n = 181), while Product-Service System innovation projects found the cards least useful (mean = 3.65, sd = 1.02, n = 75). The differences in perceived utility between project types, however, were not statistically significant (Kruskal-Wallis test, $p > 0.05$).

Examining differences between teams of each project type (Fig. 4), we note that as aforementioned, Team 7 exhibited significant differences from

others (Kruskal-Wallis test with post-hoc Dunn test, $p < 0.05$). Among product-service system project teams, no significant difference was found (Student's t-test, $p > 0.05$). Among spatio-social project teams a significant difference was found (Kruskal-Wallis test, $p < 0.05$), and a post-hoc analysis revealed Team 2 to be significantly different than other spatio-social teams (Dunn test, $p < 0.05$). Examining differences by cybersecurity risk (Fig. 5), we detect no significant pairwise differences (Kruskal-Wallis test with post-hoc Dunn test, $p > 0.05$). However, we note that projects with the least cybersecurity risk had the highest average perceived utility from the cards.

Discussion

The cards were shown to be perceived as helpful aids to the overall design process for the entire cohort of designers, given an above-positive class average assessing perceived usefulness. We find this result promising to support a hypothesis in response to our original RQ1: that card-based interventions to support cybersecurity's integration across discrete phases of the design process, organized by creativity mode, could be an effective way to support novices as they design for cybersecurity.

In response to our RQ2, however, we find inconclusive results. First, we cannot determine with confidence how card interventions are differentially perceived to be useful, whether organized by creativity mode, design phase, or intervention itself. This owes to insignificant differences in data organized by creativity mode, design phase, or card intervention outlined previously. However, the lack of a significant difference leads us to revise our hypothesis: that card interventions are perceived as equally helpful across the entire design process.

We do identify significant differences in results in response to our RQ3. While we did discover that a team focused on a product innovation project found greater average usefulness than other teams, other product innovation project teams did not exhibit notably high nor consistent perceived utility scores. Similarly, among teams pursuing spatio-social innovation projects, there was a significant difference between team two, suggesting that within the same project type, perceived utility of the card intervention could vary significantly. The differences between perceived utility by project type were not significant, however.

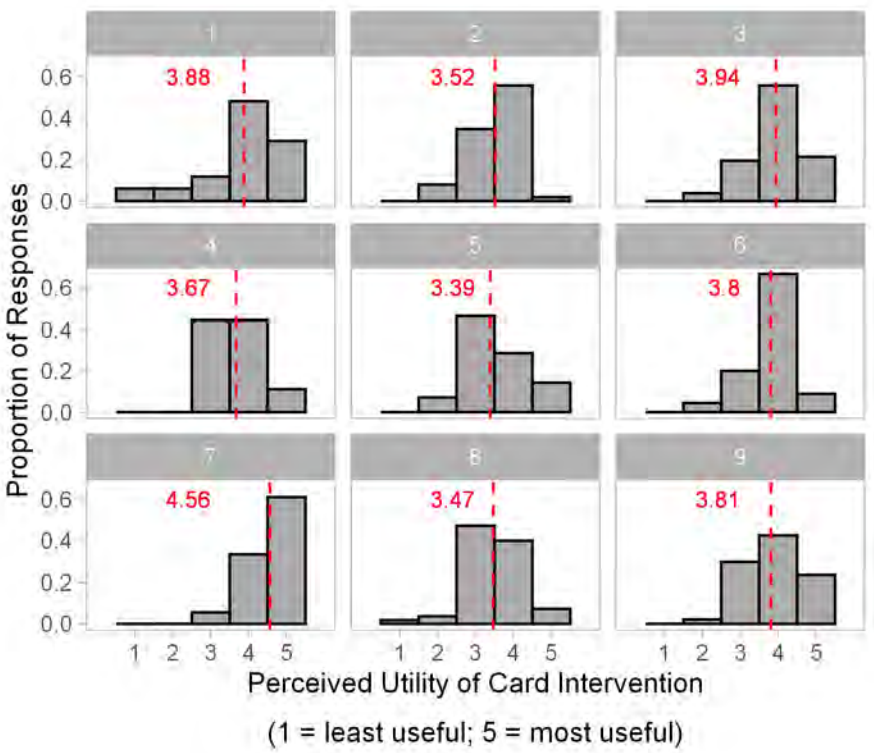
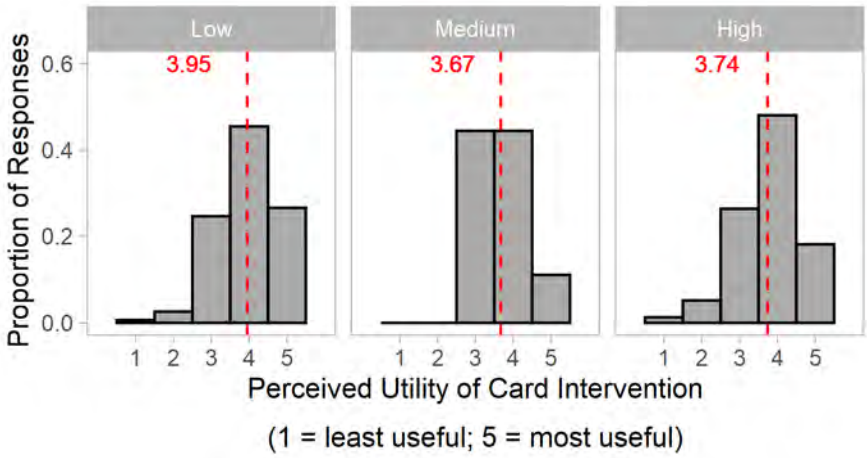


Fig. 3 Perceived utility of all card-based interventions, by project team. Team numbers, shown above each graph, are matched to project topics in Table 1.

Results related to RQ2 suggest several interesting directions for inquiry. Regarding the lack of a discrete effect from a single card, this suggests that longitudinal intervention across a design project may be superior to discrete interventions at specific phases, creativity modes, or intersections of the two. Further research on this topic could deepen the design community's understanding of the nature of process support, and under what conditions discrete support is superior to longitudinal, and vice versa.



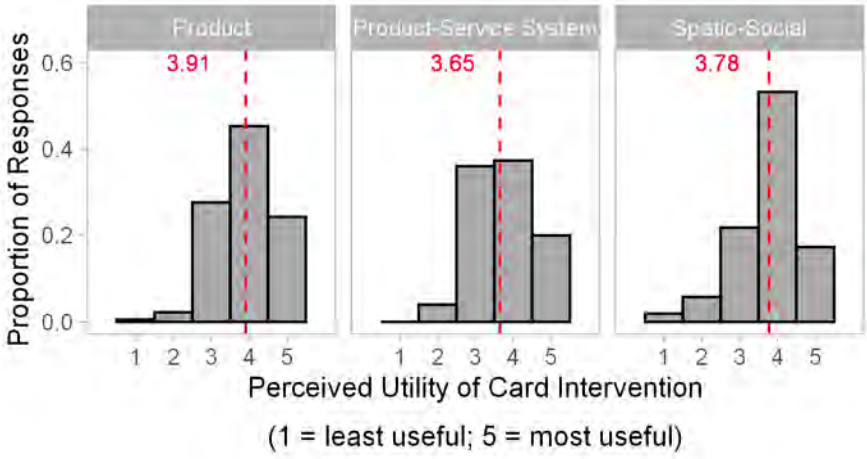


Fig. 5 Perceived utility of all card-based interventions, by cybersecurity risk.

We are intrigued by the lack of significant difference of perceived utility between project types in this study, as evidenced in RQ3. That product innovation teams and spatio-social teams find equal utility in cybersecurity support suggests that novice designers value cybersecurity process support, even if such support may not be relevant to their designs. For example, Team 7 was pursuing a project around the future of tableware and cutlery, and their final prototype was a physical set of utensils with no digital element. While there is no evident overlap of cybersecurity with the team's final prototype direction, it is interesting that the designers found cybersecurity support to be valuable throughout the design process, even if it had little evident impact

on their final prototype. Among spatio-social teams, Team 2 developed a system to safely assign work spaces in shared facilities. Unlike other spatio-social projects, 'safety' was explicitly the team's goal, leading us to speculate this was a driver of increased perceived utility, though the exact drivers are unknowns. However, the exact drivers remain unknown.

This finding is further bolstered by the lack of significant difference between project teams' perception of the cards' utility when examined by relevance of cybersecurity to the project. Our results suggest that even with minimal influence on the design *outcome or topic*, cybersecurity is a topic students find significantly useful in design *practice*. We speculate that cybersecurity's appeal to design students is grounded in provoking other paradigms of thinking about the team's project. Furthermore, as our sample size was limited to novice (student) designers, students might be finding relevance of our design interventions in other aspects of their design work. As cybersecurity concerns continue to permeate products, services, and experiences, we plan to continue to explore how interventions like the DfC cards can support designers' awareness of cybersecurity in future work.

Implications for Including Cybersecurity in the Design Process

As described earlier, there is pressing need to integrate cybersecurity into the design process. The results here aim to begin a discussion on *how* to do so, and highlight two immediate implications. First, the concept of cybersecurity appears to offer a helpful influence on human-centered design projects of a range of types and topics. As a relatively new topic for many designers, cybersecurity may be valuable content to deliver in absolute. Second, given the lack of significance in differences between cards and perceptions thereof, we suspect that a question-based modality does not allow designers enough engagement to differentiate between design interventions. We expect that questions must be supplemented with curated exercises and content to create more differentiable value for designers.

Limitations

This study has several important limitations. First, the card-based interventions were examined in a linear design process in a classroom. In contrast, much of design practice is nonlinear. Second, participants had significant autonomy in how to engage with cards, and our measurements of perceived utility are sensitive to external factors, like team dynamics. Third, we did not capture qualitative evaluations of the cards themselves, e.g., student explanations of why they used the cards, essential data for deeper conclusions. Finally, we did not examine the quality of designs, nor evaluate the presence

of pro-cybersecurity features in final designs. We are actively seeking to pursue studies resolving all of the above in future work.

Conclusions

This work presents Design for Cybersecurity (DfC) cards based on an engineering creativity model to help designers engage with cybersecurity in human-centered projects. Each card stimulates designers' creativity in a specific design phase, and fifteen cards were produced and studied in a longitudinal participant in a project-based course. The cards were perceived to have utility by participants, and while differential utility between projects or phases could not be determined with statistical significance, our findings invite further study.

Acknowledgements

The research team gratefully acknowledges support from the Center for Long-Term Cybersecurity (UC-Berkeley).

References

1. Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber Security Threats to IoT Applications and Service Domains. Wirel Pers Commun 95:169–185
2. Suo D, Siegel JE, Sarma SE (2018) Merging safety and cybersecurity analysis in product design. IET Intell Transp Syst 12:1103–1109
3. Abomhara M, Ien GMK (2015) Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. J Cyber Secur Mobil 4:65–88
4. Williams PA, Woodward AJ (2015) Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices Auckl NZ 8:305–316
5. Reid SE, Brentani UD (2004) The Fuzzy Front End of New Product Development for Discontinuous Innovations: A Theoretical Model. J Prod Innov Manag 21:170–184
6. Zhang Q, Doll WJ (2001) The fuzzy front endand success of new product development:a causal model. Eur J Innov Manag 4:95–112

7. Roschuni C, Kramer J, Agogino A (2016) Design Talking: How Design Practitioners Talk About Design Research Methods. https://doi.org/10.1115/DETC2015-47843
8. Roschuni C, Kramer J, Zhang Q, Zakskorn L, Agogino A (2015) Design Talking: An Ontology of Design Methods to Support a Common Language of Design. Proc. Int. Conf. Eng. Des.
9. Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M (2018) The Evolving State of Medical Device Cybersecurity. Biomed Instrum Technol 52:103–111
10. Yuan X, Yang L, Jones B, Yu H, Chu B-T (2016) Secure software engineering education: Knowledge area, curriculum and resources. J Cybersecurity Educ Res Pract 2016:3
11. Lukowiak M, Radziszowski S, Vallino J, Wood C (2014) Cybersecurity education: Bridging the gap between hardware and software domains. ACM Trans Comput Educ TOCE 14:2
12. Assal H (2018) The Human Dimension of Software Security and Factors Affecting Security Processes. Text, Carleton University
13. Navas J, Voirin J-L, Paul S, Bonnet S (2019) Towards a Model-Based approach to Systems and Cyber Security co-engineering. INCOSE Int Symp 29:850–865
14. Hatchuel A, Chen MK (2017) Creativity under Strong Constraints: the Hidden Influence of Design Models. Eur Rev 25:194–207
15. Islam T, Becker I, Posner R, Ekblom P, McGuire M, Borrion H, Li S (2019) A Socio-Technical and Co-evolutionary Framework for Reducing Human-Related Risks in Cyber Security and Cybercrime Ecosystems. In: Wang G, Bhuiyan MZA, De Capitani di Vimercati S, Ren Y (eds) Dependability Sens. Cloud Big Data Syst. Appl. Springer, Singapore, pp 277–293
16. Yilmaz S, Christian JL, Daly SR, Seifert C, Gonzalez R (2012) How do design heuristics affects outcomes? In: 70 Proc. Des. 2012 12th Int. Des. Conf. Dubrov. Croat. pp 1195–1204
17. Yilmaz S, Seifert C, Daly SR, Gonzalez R (2016) Design Heuristics in Innovative Products. J Mech Des. https://doi.org/10.1115/1.4032219
18. Method Cards. https://www.ideo.com/post/method-cards. Accessed 30 Nov 2019
19. AI & Ethics: Collaborative Activities for Designers. https://www.ideo.com/post/ai-ethics-collaborative-activities-for-designers. Accessed 30 Nov 2019
20. Superpowers Card Deck. In: SYPartners. https://madeby.sypartners.com/products/superpowers-card-deck. Accessed 30 Nov 2019

21. drivers of change digital app for iOS and Android. http://www.driversofchange.com/. Accessed 30 Nov 2019
22. (2019) IDC Design Method Card. In: SUTD-MIT Int. Des. Cent. https://idc.sutd.edu.sg/design-contributions/creations/idc-design-method-card. Accessed 30 Nov 2019
23. Deng Y, Antle AN, Neustaedter C (2014) Tango Cards: A Card-based Design Tool for Informing the Design of Tangible Learning Games. In: Proc. 2014 Conf. Des. Interact. Syst. ACM, New York, NY, USA, pp 695–704
24. Brandt E, Messeter J (2004) Facilitating Collaboration Through Design Games. In: Proc. Eighth Conf. Particip. Des. Artful Integr. Interweaving Media Mater. Pract. - Vol. 1. ACM, New York, NY, USA, pp 121–131
25. Halskov K, Dalsgaard P (2006) Inspiration Card Workshops. In: Proc. 6th Conf. Des. Interact. Syst. ACM, New York, NY, USA, pp 2–11
26. Wölfel C, Merritt T (2013) Method Card Design Dimensions: A Survey of Card-Based Design Tools. In: Kotzé P, Marsden G, Lindgaard G, Wesson J, Winckler M (eds) Hum.-Comput. Interact. – INTERACT 2013. Springer, Berlin, Heidelberg, pp 479–486
27. Lauff CA, Perez KB, Camburn BA, Wood KL (2019) Design Principle Cards: Toolset to Support Innovations With Additive Manufacturing. In: Vol. 4 24th Des. Manuf. Life Cycle Conf. American Society of Mechanical Engineers, Anaheim, California, USA, p V003T05A005
28. Yilmaz S, Seifert CM (2011) Creativity through design heuristics: A case study of expert product design. Des Stud 32:384–415
29. Hasling KM, Ræbild U (2017) Sustainability Cards: Design for Longevity. PLATE 2017 Prod. Lifetimes Enviroment
30. Ræbild U, Hasling KM (2018) Sustainable Design Cards: A Learning Tool for Supporting Sustainable Design Strategies. Sustain Fash Circ Econ 128–151
31. Lucero A, Arrasvuori J (2010) PLEX Cards: A Source of Inspiration when Designing for Playfulness. In: Proc. 3rd Int. Conf. Fun Games. ACM, New York, NY, USA, pp 28–37
32. Kim E, Jensen MB, Poreh D, Agogino AM (2018) Novice Designers' Lack of Awareness to Cybersecurity and Data Vulnerability in New Concept Development of Mobile Sensing Devices. 92 Proc Des 2018 15th Int Des Conf. https://doi.org/10.21278/idc.2018.0461
33. Kim E, Kwon J, Yoon J, Agogino AM Embedding Cybersecurity Into Design Education: Increasing Designers' Awareness of Cybersecurity Throughout the Design Process. ASME 2019 Int. Des. Eng. Tech. Conf. Comput. Inf. Eng. Conf.

34. Mouheb D, Abbas S, Merabti M (2019) Cybersecurity Curriculum Design: A Survey. In: Trans. Edutainment XV. Springer, pp 93–107
35. Luburić N, Sladić G, Slivka J, Milosavljević B (2019) A Framework for Teaching Security Design Analysis Using Case Studies and the Hybrid Flipped Classroom. ACM Trans Comput Educ TOCE 19:21
36. Huynh D, Luong P, Iida H, Beuran R (2017) Design and Evaluation of a Cybersecurity Awareness Training Game. In: Munekata N, Kunita I, Hoshino J (eds) Entertain. Comput. – ICEC 2017. Springer International Publishing, pp 183–188
37. Cards. In: Cyber Realm. https://gencybercards.com/cards. Accessed 30 Nov 2019
38. Jin G, Tu M, Kim T-H, Heffron J, White J (2018) Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. J Educ Learn EduLearn 12:150
39. Chu ES, Payne A, Seo JH, Chakravorty D, McMullen D (2019) Data Center Physical Security Training VR to Support Procedural Memory Tasks. In: Stephanidis C (ed) HCI Int. 2019 - Posters. Springer International Publishing, pp 353–358
40. Coles-Kemp L (2009) Information security management: An entangled research challenge. Inf Secur Tech Rep 14:181–185
41. Coles-Kemp L, Ashenden A (2012) Community-centric engagement: lessons learned from privacy awareness intervention design. In: 26th BCS Conf. Hum. Comput. Interact. 26. pp 1–4
42. Coles-Kemp L, Theoharidou M (2010) Insider threat and information security management. In: Insid. Threats Cyber Secur. Springer, pp 45–71
43. Lewis MM, Coles-Kemp L (2014) Who says personas can't dance? The use of comic strips to design information security personas. In: CHI14 Ext. Abstr. Hum. Factors Comput. Syst. pp 2485–2490
44. Denning T, Shostack A, Kohno T (2014) Practical lessons from creating the control-alt-hack card game and research challenges for games in education and research. 2014 USENIX Summit Gaming Games Gamification Secur. Educ. 3GSE 14
45. Denning T, Lerner A, Shostack A, Kohno T (2013) Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In: Proc. 2013 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS 13. ACM Press, Berlin, Germany, pp 915–928
46. Home | The Security Cards: A Security Threat Brainstorming Kit. http://securitycards.cs.washington.edu/index.html. Accessed 30 Nov 2019

47. Nick Merrill. https://cosmopol.is/adversary-personas/. Accessed 30 Nov 2019
48. Howard T, Culley SJ, Dekoninck E (2007) Creativity in the Engineering Design Process. 42 Proc. ICED 2007 16th Int. Conf. Eng. Des. Paris Fr. 28-31072007
49. Howard TJ, Culley SJ, Dekoninck E (2008) Describing the creative design process by the integration of engineering design and cognitive psychology literature. Des Stud 29:160–180
50. Gero JS, Kannengiesser U (2004) The situated function–behaviour–structure framework. Des Stud 25:373–391
51. Sultan, Ahmad (2019) Report: Improving Cybersecurity Awareness in Underserved Populations - CLTC UC Berkeley Center for Long-Term Cybersecurity.
52. Ceschin F, Gaziulusoy I (2016) Evolution of design for sustainability: From product design to design for system innovations and transitions. Des Stud 47:118–163
53. Reniers G, Khakzad N, Gelder PV (2017) Security Risk Assessment: In the Chemical and Process Industry. Walter de Gruyter GmbH & Co KG