Proceedings of the ASME 2019
International Design Engineering Technical Conferences
and Computers and Information in Engineering Conference
IDETC/CIE2019
August 18-21, 2019, Anaheim, CA, USA

IDETC2019-97720

EMBEDDING CYBERSECURITY INTO DESIGN EDUCATION: INCREASING DESIGNERS' AWARENESS OF CYBERSECURITY THROUGHOUT THE DESIGN PROCESS

Euiyoung Kim
Industrial Design Engineering, Delft University of Technology, Delft, NL
Jacobs Institute for Design Innovation, University of California at Berkeley, Berkeley, CA, US

Jieun Kwon
Human Factors and Ergonomics
University of Minnesota
Minneapolis, MN, US

JungKyoon Yoon
Design and Environmental Analysis
Cornell University
Ithaca, NY, US

Alice M. Agogino
Mechanical Engineering
University of California at Berkeley
Berkeley, CA, US

ABSTRACT

As more digital devices with sensing capabilities are introduced into users' daily lives, the risks of threats to data and privacy and security have increased. While cybersecurity has been acknowledged as an important concern in developing products with digital services, currently available design methodologies and practices offer limited effective guidance to designers to explicitly address cybersecurity issues. In this paper, we present a case study from a product design course at the University of California, Berkeley, where the course's teaching team implemented an intervention in the form of cybersecurity-focused educational materials into the design process. The baseline and post-intervention survey results indicate that the cybersecurity intervention throughout the course had positively influenced the students' awareness of cybersecurity ($p<0.001$, $SD=0.79$, 26% increase in score, Cohen's $d=0.81$). The intervention provoked the designers to consider and include aspects of cybersecurity in developing their design solutions throughout most of the design process. However, their increased awareness aside, the extent of the student teams considering cybersecurity had tapered off over the 6-week design course with little noticeable influence in the final design.

Keywords: cybersecurity awareness, design education, design process, user-centered design, case study

1. INTRODUCTION

Mobile sensing devices are predicted to have exponential growth in multiple domains, ranging from surveillance, connected homes, and video games to car-sharing services [1,2]. While these new devices have provided a variety of unprecedented, convenient functions, the utilization of new sensing technologies is not without risk [3,4]. Aiming only at incorporating them into products without holistically considering the impacts on users can potentially hinder users' well-being.

A number of incidents have been reported in which users' cybersecurity and privacy had been disrupted. For example, certain classified military data, i.e., locations of individuals, were inadvertently exposed because of a commercial wearable device worn by patrol soldiers [5]. Users often unknowingly consent to their smart home devices continuously collecting and making use of their data, e.g., their voice calls and video monitoring. This can sometimes be attributed to the devices' ambiguous installation instructions. In one well-known case, Amazon devices were found to be frequent targets of hackers: Amazon's Alexa—the voice-controlled smart speaker—recorded private conversations and then sent the file to random contacts [6].

We postulate that apart from users' insensitivity to careful data management and limited training, one of the main reasons for the incidents mentioned above is designers' lack of awareness of cybersecurity and privacy risks when developing their products [7]. In other words, users' safe product use in terms of cybersecurity has not been adequately addressed upfront in the design process (e.g., in the design conceptualization and evaluation phases). As a consequence, the majority of digital devices with sensing capabilities fall short of the standards in protecting users' security and privacy [8]. The security of user data may not be robustly protected when the intention to keep user data safe remains unstated in the design process, which can result in unforeseen or unwanted user behavior, leading to data breaches and hacking. This implies that stimulating designers to be aware of cybersecurity issues throughout the design process

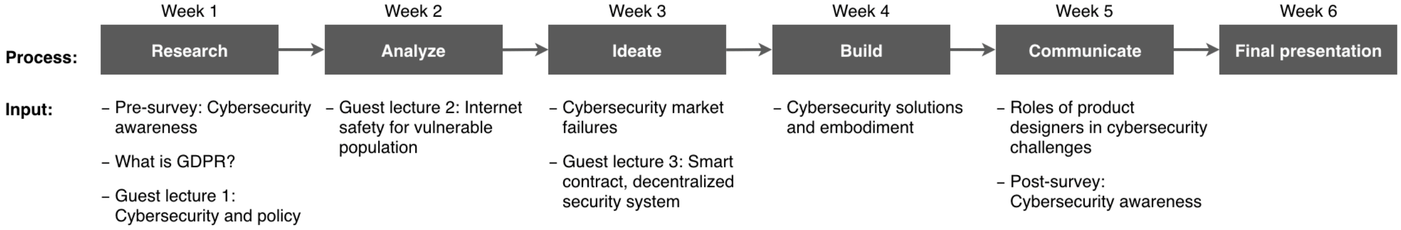
Week 1
Week 2
Week 3
Week 4
Week 5
Week 6
Process:
Research
Analyze
Ideate
Build
Communicate
Final presentation
Input:
– Pre-survey: Cybersecurity awareness
– What is GDPR?
– Guest lecture 1: Cybersecurity and policy
– Guest lecture 2: Internet safety for vulnerable population
– Cybersecurity market failures
– Guest lecture 3: Smart contract, decentralized security system
– Cybersecurity solutions and embodiment
– Roles of product designers in cybersecurity challenges
– Post-survey: Cybersecurity awareness

FIGURE 1: CYBERSECURITY INTERVENTIONS OVER A 6-WEEK DESIGN COURSE

can be critical to developing products that are secure against potential risks.

Education about privacy, data protection, and cybersecurity has been emphasized within the domains of computer science and engineering; for an overview, see [9,10]. However, little of the literature addresses the topics as an essential quality of product design and development, even though more digital/tech companies have been struggling with an increasing number of cybersecurity issues from more digitalized devices being interconnected in recent years [11]. Despite the problem's significance, recent research shows that cybersecurity education in the U.S. has not adequately changed the students' cybersecurity awareness mindsets [12,13]. Moreover, recent cybersecurity campaigns have not led to increased user cybersecurity awareness or desirable behavioral changes [14]. Taken together, these suggest that little viable knowledge is available to assist designers in their attempts to minimize cybersecurity risks in user experiences.

According to Kim, Jensen, and Agogino [15], implicit interventions[1] (e.g., verbalized prompts to ask students to take cybersecurity into consideration as well as team check-ins) were not effective enough to inculcate designers against cybersecurity issues and stimulate them to pay attention to user privacy and data protection in developing design concepts. This paper builds on their previous study, with the aim of exploring how designers' awareness of cybersecurity can be increased in the context of design education. In particular, we focused on how educational curricula and materials can effectively be implemented and embedded into design education. Thus, this research addresses the question: *how can designers be supported to consider cybersecurity, through educational curricula and materials?*

The answers to this question were explored within the setting of an undergraduate design course utilizing a series of educational materials. The paper begins by introducing the course setting and the applications of the educational curriculum and materials. Next, their effectiveness in increasing designers' cybersecurity awareness is reported through baseline and post-surveys. Then, the changes in awareness levels throughout the design process are described, which were examined by analyzing the students' weekly reports and final design outcomes. On the basis of the findings, some implications for design education and the development of design support (e.g., design methods and tools) are discussed, along with several proposals for future research.

2. DESIGN CASE—DESIGN FOR CYBERSECURITY AND DATA PROTECTION

The design case that is hereafter reported was conducted in a six-week project-based design course at the University of California, Berkeley: DesInv. 290T—Human-Centered Design: Reimagining Sensing and Mobility. The course revolved around a collaborative design challenge ("reimagining mobile sensing and mobility") with a focus on cybersecurity, privacy, and data protection. Twenty-eight undergraduate students took the course: their educational backgrounds varied, to include design, data science, mechanical engineering, economics, and architecture. The students were split into six teams of four (or five) students, and each team worked on a different design challenge (e.g., a real-time remote monitoring system for child–parent interaction and a digital navigation system for public transportation).

Research approach. Two main research methods were used: (1) action research to implement cybersecurity education in a course and (2) an intervention study that used an online survey to measure the changes to designers' cybersecurity awareness as the course progressed. The applications of these two methods are described in the following sections.

2.1 Action research

Procedure. We conducted action research [17,18] in the design course to make the course curriculum and structure into an explicit intervention. The course comprised five design phases—research, analyze, ideate, build, and communicate—based on the design process developed by *theDesignExchange* [19]. Over the six weeks, several inputs—e.g., cybersecurity topic lectures, a new General Data Protection Regulation (GDPR)[2], and case studies—were offered to the students, each followed by a discussion, in which students shared their lessons learned and implications for their projects. Figure 1 visualizes the course process and inputs.

Data analysis. We reviewed the written data, collected in the form of team-level weekly reports. Every week, over six weeks in total, the students submitted their weekly reports summarizing the project's progress to date and describing their reflections.

[1] The implicit curriculum did not include explicit design guidelines on cybersecurity, rather it was crafted within the individual teacher's prompts in homework, exercises and design reviews. For a detailed discussion of implicit and explicit curricula, see [16].

[2] The EU General Data Protection Regulation (GDPR), https://eugdpr.org

TABLE 1: EXAMPLE SENTENCES IN THE REPORT REPRESENTING EACH ATTENTION LEVEL

Level	Evaluation Criteria	Example Sentences
High (3)	Cybersecurity is explicitly addressed in a weekly report (e.g., data collection, analysis of observational research, potential design directions or product features)	*It is important to look into how people at concerts secure their data-sensitive belongings, particularly credit/debit cards and cell phones. It may be a good opportunity to look into physical ways we can help protect these users by securing their data-sensitive belongings in a rowdy environment such as concerts and music events.* – Team 1's week 1 report
Medium (2)	Cybersecurity is somewhat addressed in a weekly report, yet the report misses details and supporting evidence	*We decided that the features to be added to our product would be: voice activation, a remote of some sort to allow mute individuals to use this product, and two iterations of the product. The first iteration would allow for Internet and Bluetooth connectivity. The second iteration would provide a repository for local memory, to protect the user's personal data.* – Team 4's week 6 report
Low (1)	Cybersecurity issues are hardly considered as a primary discussion	*Updated, real-time data is provided to users who wish to access the information. Concerns over this program include privacy issues as the locations of individuals may be exposed.* – Team 5's week 1 report
None (0)	Cybersecurity issues not addressed	No example sentences: no evidence of cybersecurity related words is provided in a report.

The students were instructed to justify the design methods they used and include their reflections on how they considered cybersecurity in the process. In total, 30 reports were collected, which were anonymized for data analysis.

The data-sets were reviewed by two experts experienced in design education and user-centered design research. The reviewers independently examined the degree to which the student teams considered and included aspects of cybersecurity into the design process. The attention levels to cybersecurity awareness were rated on a four-point scale (high, medium, low, and none). The two reviewers' ratings were compared. In case of disagreement, they revisited and discussed the data, and iteratively moderated the ratings. Examples of sentences in analyzed reports that represent each attention level are presented in Table 1.

Results. The heatmap in Figure 2 visualizes the levels of cybersecurity awareness of each team over the six weeks (horizontal axis: teams 1-6; vertical axis: weeks 1-6). The four levels of awareness were color coded: the darker the color, the higher the cybersecurity inclusiveness. Team 1 was the only group that had consistent (μ=3, highest levels: 3 out of 0-3 on the four-point scale) degree of cybersecurity awareness throughout the design process; they kept considering cybersecurity throughout the project preparation, data collection, analysis of observational research, prototyping, and communication.
For example, their report in the research phase (week 1) addresses:

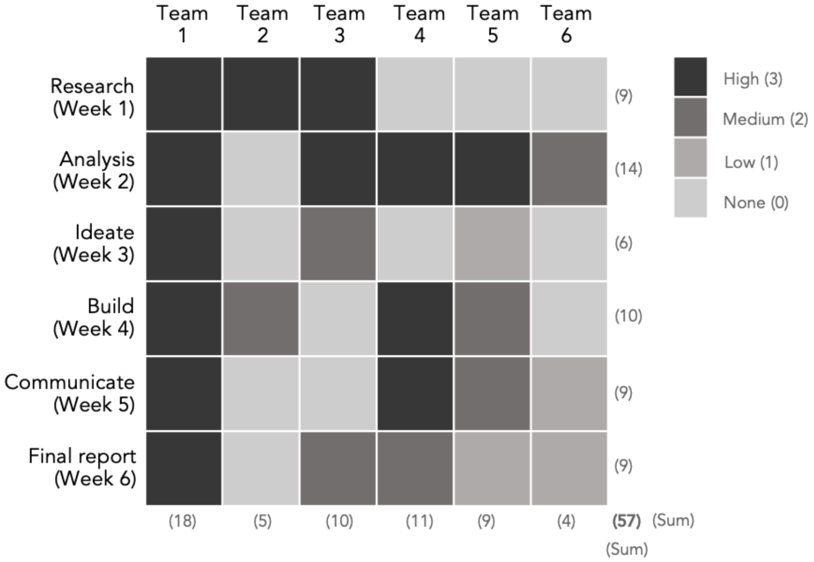

FIGURE 2: CHANGES IN CYBERSECURITY AWARENESS LEVELS OF THE SIX TEAMS OVER SIX WEEKS: SCORES OF 0 (NONE: LIGHT GREY) TO 3 (HIGH: DARK GREY)

> We've decided that researching music event goers would be a good opportunity to see how such users secure their data-sensitive belongings in active, sometimes rowdy environments such as concerts. Looking into how they deal with cyber security and privacy will be important as well.

In contrast to Team 1, Team 6 demonstrated the least amount of cybersecurity inclusion (μ=0.67). Although their research activities covered the topic of cybersecurity, the team did not further investigate the users' underlying concerns or related issues, even when participants vocalized their privacy concerns. While their interview script addressed cybersecurity inclusion in both the interview questions and the participants' responses, for instance, no further consideration of cybersecurity followed in the next design phases.

> "[…] *You are the first parent to bring up that topic of privacy.* […] *You also mentioned that you were not so comfortable sharing your kid's pictures online. Why is that, if I may ask?"* (excerpted from Team 6's week 2 report)

The analyze design phase (week 2) had the highest cybersecurity attention score (the sum of the entire teams' awareness level=14). For instance, the report of Team 3 illustrated the heightened awareness that described the HMW[3] (how might we?) method implementation:

> *"We are going to focus on thinking about how location data, transportation, and cybersecurity can come together for a greater good and help more people while also being more secure by addressing the following questions:*
>
> *(a) How might we improve the link between cybersecurity and transportation?*
>
> *(b) How might we utilize cybersecurity in a way that impacts users on the go?*
>
> *(c) How might we teach users about cybersecurity?*
>
> *(d) How might we find need for users to understand cybersecurity on the go?*
>
> *(e) How might we allow customers to use cybersecurity for their own benefit?*
>
> *(f) How might we allow customers to protect themselves with cybersecurity?"* (excerpted from Team 3's week 2 report)

We found that teams 4, 5, and 6 also incorporated cybersecurity in different perspectives in week 2, markedly reporting data analysis results and team reflection built on the research in the previous phase.

The most noteworthy observation is that in general, the extent of considering cybersecurity tapered off over time by the final phase of the process, especially in the design implementation and communication phases. Speaking of the changes to the color gradations shown in Figure 2, while some teams (e.g., Teams 3 and 4) addressed cybersecurity in the early design process, the degree of the inclusion decreased over time. Overall, the average cybersecurity awareness scores in the first week and the final week, taken from all teams, were the same (μ=1.5 in both occurrences).

2.2 Online surveys

Procedure. Two surveys were conducted (baseline and post-course) that measured each student's basic exposure to electronic devices and her/his understanding of cybersecurity before and after the intervention (see the inputs described in Figure 1). The two surveys equally consisted of six items on individual device use patterns (e.g., "On average, how frequently do you use your device?" and "On average, how many people do you share your device with?"), a five-item Likert scale on cybersecurity awareness level (e.g., "On a scale of 1 to 5, how familiar are you with the term cybersecurity?" and "On a scale of 1 to 5, how much do you consider cybersecurity in the product design processes?"), and three items on basic demographics such as gender and major. Among the 28 students, 22 individuals completed both the baseline and post-surveys (male: 13, female 9).

Data analysis. For the device use pattern survey, a simple numeric comparison between the baseline and post-course device use pattern was done. For the cybersecurity awareness survey, the data collected for each survey item were averaged as "overall cybersecurity score", and the differences in mean values between the baseline and post-course surveys were compared. In order to ensure that the baseline and post-intervention groups matched, we eliminated the data of participants who did not complete both of the surveys.

Results. The results of the two surveys were summarized into three parts: the device use pattern comparison, the cybersecurity awareness comparison, and the comparison of future intentions. First, Table 2 summarizes the results of the device use patterns in baseline and post-surveys.

TABLE 2: BASELINE AND POST-CYBERSECURITY DEVICE USE PATTERN SURVEYS

Questions	Choice	Baseline	Post
Device share with others	Nobody. I use all devices by myself	4	3
	1-2 people	12	14
	3-5 people	6	4
Device use frequency per week	Less than 5 times	1	1
	5-20 times	5	9
	More than I can count	16	12
Do not allow device to collect personal data	Yes	2	8
Do not feel comfortable with data collection	Yes	10	16
Voluntarily studied cybersecurity outside classroom	Yes	9	11

[3] How Might We? Methods, https://www.thedesignexchange.org/design_methods/342

Overall, the comparison of the two surveys indicates an improvement in cybersecurity prevention through device use patterns among students throughout the course. Two of the participants who shared their device with 3–5 people changed to sharing their device with 1–2 people. The number of participants who were willing to provide their personal information decreased when the device asked them to collect personal data (two to eight individuals). Similarly, the number of participants who felt uncomfortable giving their information to the device increased (from 10 to 16). Additionally, the number of participants who voluntarily studied cybersecurity slightly increased (from nine to 11).

In the second part of the analysis, the results showed increased cybersecurity awareness throughout the course (see Table 3).

TABLE 3: FIVE-ITEM BASELINE AND POST-CYBERSECURITY AWARENESS SURVEYS (SCORES OF 0-5)

Choice	Baseline	Post
How familiar are you with cybersecurity?	2.68	3.90
How concerned are you with cybersecurity?	3.91	4.32
How important is cybersecurity in the design process?	4.27	4.41
How much do you consider cybersecurity when purchasing a product?	3.00	4.29
How much do you consider cybersecurity when designing a product?	3.09	4.36
Overall Cybersecurity Score	**3.39**	**4.26**

A simple t-test that compared the pre-and post-surveys' results showed that the difference between the two data sets was significant for the *overall cybersecurity score ($p^{**}<0.001$, SD=0.79, 26% increase in score, Cohen's d=0.81),* for which cybersecurity awareness increased significantly from a baseline (M=3.39, SD = 1.24) to post (M=4.26, SD = 0.84). The change from baseline to post-intervention was especially large regarding how much the students considered cybersecurity when purchasing a product. The t-test revealed a significant increase in cybersecurity awareness among the participating design students before and after the intervention courses. In particular, the increase in awareness was especially strong for familiarity with cybersecurity (46% increase in score), cybersecurity considerations when purchasing a new product (43% increase in score), and consideration when designing a product (41% increase in score).

In the third part of the analysis, we examined the answers from one of the survey questions: "Which of the following information would you provide the device?". This future-intentions-survey question results revealed that the number of individuals willing to give information about their location, health information, contact information, and address had noticeably decreased after the course intervention (see Table 4).

Also, an additional question on future-intentions showed that the participants' desire to improve the device had also shifted from focusing on the device's functionality to cybersecurity.

TABLE 4: THE RESPONSES TO THE QUESTION "WOULD YOU GIVE THIS INFORMATION?": THE FUTURE INTENTIONS SURVEY RESULTS

	Baseline (Pre-) N	Post-survey N	(Post N – Baseline N)
Name	14	14	(0)
Gender	18	18	(0)
Weight	5	6	(+1)
Height	6	8	(+2)
Location (GPS)	10	3	(-7)
Health info	3	0	(-3)
Photos, videos	7	4	(-3)
Contact email	13	7	(-6)
Address	4	0	(-4)

N= The number of people who would allow the device to collect that information

For example, for the question asking what the participants would improve with their device (before intervention), they answered, "faster Internet connection," "elongated battery life," and "larger storage space" in the baseline survey. These answers then changed to "more security and less advertisements," "camera and microphone security," and "improved user control" in the post-intervention survey.

In a sense, the increased sensitivity to cybersecurity was translated into possible future digital device purchase and usage behaviors (e.g., not giving personal information when the device asks for it and thinking about cybersecurity improvements for the existing product).

3. DISCUSSION

In this research, we explored how students' awareness of cybersecurity issues can be stimulated within the setting of a design course utilizing a series of educational curricula and materials. Their effectiveness in increasing designers' cybersecurity awareness was examined through baseline and post-surveys. Then, the changes to awareness levels throughout the design process were examined by analyzing the students' weekly reports and final design outcomes. In this section, we report on challenging discussion points as results of our study: (1) the contrast between the cybersecurity awareness survey and the action research results in the product design and (2) the comparison of cybersecurity attention levels between Team 1 and the rest teams. We end with the need to develop and integrate a set of explicit cybersecurity criteria into the design process.

Contrast between the cybersecurity awareness survey and action research results. Despite the small sample size, the results of the baseline and post-surveys suggest that the in-class cybersecurity subject inputs successfully increased the students' awareness. However, the level of attention gradually decreased over time. The two studies' results raise the following question: *does increased cybersecurity awareness practically help designers to address cybersecurity issues in the design process?*

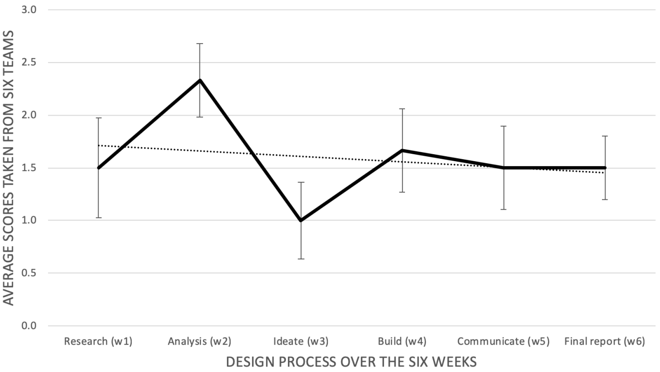

FIGURE 3: CYBERSECURITY AWARENESS LEVEL TREND: AVERAGE SCORES TAKEN FROM THE SIX TEAMS OVER SIX WEEKS

In other words, *does a designer with a highly developed sensitivity to cybersecurity indeed develop secure products?* To answer this question, we reexamined the students' weekly reports, giving attention to the changes in cybersecurity considerations among students throughout the course, which is visualized in Figure 3. The chart was formulated based on the average cybersecurity awareness ratings of the six teams (for the details of the data collection and analysis, see Section 2.1).

Note that the chart is intended to offer a general impression of the changes to awareness levels, instead of statistically comparing the differences. The chart indicates that the incorporation of cybersecurity concepts was highest in the analysis stage and then dropped to the lowest point during the ideation phase. Although a t-test on the cybersecurity awareness survey revealed a statistically significant increase to awareness at the end of the course, it seems that this increased awareness was not fully reflected throughout the design process. For example, Team 2 formulated a list of guiding questions to address cybersecurity challenges in their concept development in week 2, such as (1) "How might we improve the link between cybersecurity and transportation?" and (2) "How might we train users' cybersecurity sensitivity?" However, the plan and action items in the later stages neglected to investigate cybersecurity challenges, and the final design outcomes hardly reflected any detailed issues of cybersecurity.

In fact, the trend line (the dotted line in Figure 3) shows that the incorporation of cybersecurity into design processes had actually fallen from weeks 1 to 6. This implies a discrepancy between individual cybersecurity awareness and its practical design application. Thus, how can cybersecurity issues be explicitly taken into account in the design process, and how can their salience be kept and translated into design outcomes? In our view, it is important to carry out ongoing and iterative critical examinations of how the design decisions and the resulting products can be legitimate in terms of cybersecurity concerns. One strategy for this could be to include recurring cycles of reflection in the design process, during which the cybersecurity aspects of user experience and design requirements are made explicit, thereby anticipating possible risks and what needs to be done to alleviate them. For this, developing a set of cybersecurity criteria that can be used to guide the reflection and discussion processes is needed.

Comparison of cybersecurity attention levels between Team 1 and the rest teams. What is noteworthy about our research is the comparison of attention levels between team 1 and the rest of teams (Team 2 – 6). In figure 2, Team 1 was an only group that demonstrated consistent cybersecurity attention levels throughout the entire design process. While how and what is still unknown question, we found that team 1 stood out from the rest of the teams in that the team not only presented their proposed ideas to incorporate cybersecurity into the design process but they also executed them; thus the results and reflection in the reports were written in a richer and more explicit manner. Team 1's report in the final phase (week 6) delineates notable reflection on their design process with respect to the cybersecurity inclusiveness that we aim to see more from other designers in the future cybersecurity curriculum embedment:

> *"Cybersecurity is not a feature that is emphasized or discussed as often as it should be, given its ever-increasing importance in the modern digital world today. However, thinking about our users' needs and possible solutions in the context of the cybersecurity design challenge not only posed new and interesting challenges, but also underscored the fact that cybersecurity should be a consideration from the very start. Ultimately, we discovered that cybersecurity and physical security should from now on be integrated into the design process of any design project as it is important that we design to protect the privacy of people and their everyday use of products, whether those products are digital or non-digital."* (excerpted from Team 1's week 6 report)

Need to develop a set of cybersecurity criteria in design education. Several criteria for assessing certain qualities of a design (e.g., usefulness, feasibility, innovativeness, and originality) have been introduced and implemented in design research methods [20-27]. While useful for considering the general acceptability of a product, they appear to be limited in terms of helping designers to take a nuanced view of cybersecurity issues and their possible experiential impacts [28,29].

In fact, the relevance and effectiveness of having a set of cybersecurity criteria were echoed by Team 1's consistent consideration of cybersecurity throughout the design process (for details, see the level of cybersecurity awareness depicted in Figure 2). We could find that Team 1 formulated their own criteria to address cybersecurity issues and used them in appraising their design directions alongside other evaluation criteria, e.g., novelty, plausibility, and marketability. The team stated that having the criteria allowed them to put cybersecurity at the core of their project's vision and make their decisions accordingly. This signifies the relevance and importance of involving cybersecurity into the considerations within the product design process.

The need to consider cybersecurity in design evaluation criteria has already been discussed within the field of human–computer interaction (HCI) [for an overview, see, 30-33].

Johnston et al. [29] proposed putting criteria into security when designing interfaces. In line with this, Yee [28] introduced a guideline for assessing the security quality of software design, while Ibrahim et al. [30] proposed a modified version of usability heuristics integrating cybersecurity aspects of design. Despite these initiatives to create products that are both usable and secure, to our knowledge, the practical benefits of embedding the cybersecurity criteria into the design process have not yet been empirically studied. In design research, a possible research direction could be to investigate if and how incorporating cybersecurity criteria into the design process could increase the effectiveness of design outcomes in terms of cybersecurity. The resulting insights could support designers to deliberately tackle cybersecurity challenges in their practices.

4. LIMITATIONS

Our study is not without its limitations. The results presented in the current paper were systematic, but our findings are based on a single design case: the students were given the same design challenge and the final solution each team came up with varied. The awareness survey was subjective, and students might have presented normative results. The intervention methods have their own shortcomings in interpreting the outcome, especially when other elements external to the intervention course, covariates such as personality of the participants and effort devoted when reporting the design process [34]. Moreover, given the relatively small sample size of the study, we acknowledge that we should be cautious about generalizing the findings. Therefore, we invite additional case studies that could replicate the results across design briefs, samples, and intervention types.

5. CONCLUSION AND FUTURE RESEARCH

In the present research, we developed teaching materials to support design students to purposefully consider cybersecurity issues in the design process. We implemented two design methods from a product design course—cybersecurity awareness online surveys and action research—to investigate the changes to cybersecurity inclusion in the design process. The results show that the cybersecurity intervention positively influenced the students' cybersecurity awareness throughout the course. This intervention did not effectively provoke the design students to consider and include aspects of cybersecurity in developing their design solutions. The extent of the cybersecurity inclusion among most of the teams tapered off over time. Given these findings, we encourage research to further explore how designers' increased cybersecurity awareness and knowledge can be translated into the design process and design outcomes. These explorations may contribute to the development of design support (e.g., design criteria, design methods, and educational materials) to help designers and project stakeholders in their efforts to effectively address cybersecurity challenges.

ACKNOWLEDGEMENTS

This research was partially supported by a CLTC (Center for Long-term Cybersecurity) grant 2018-2019 at the University of California, Berkeley.

REFERENCES

[1] Kumar, K. "Personal Robots Market to Touch $34,120.3 Million by 2022." *P&S Market Research* (2017). URL https://globenewswire.com/news-release/2017/07/05/1038878/0/en/Personal-Robots-Market-to-Touch-34-120-3-Million-by-2022-P-S-Market-Research.html.

[2] Tao, M. "Sony Returns to Robotics Market after 12 Years Away." Robotics & Automation News (2017). URL https://roboticsandautomationnews.com/2017/10/08/sony-returns-to-robotics-market-after-12-years-away/14407/.

[3] Schneier, B. "IoT Security: What's Plan B?" *IEEE Security & Privacy* Vol. 15 No. 5 (2017): p. 96.

[4] Tweneboah-Koduah, S., Skouby, K. E., and Tadayoni, R. "Cyber Security Threats to IoT Applications and Service Domains." *Wireless Personal Communications* Vol. 95 No. 1 (2017): pp. 169–185.

[5] Hsu J. "The Strava Heat Map and the End of Secrets". *Wired* (2018). URL https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/, accessed 02/24/2019.

[6] Shaban, H. "An Amazon Echo Recorded a Family's Conversation, then Sent It to a Random Person in Their Contacts, Report Says." *The Washington Post* (2018). URL https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on&utm_term=.d53b0919b775.

[7] Williams, P. A. and Woodward, A. J. "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. *Medical Devices* (Auckland, NZ) Vol. 8 (2015): p. 305.

[8] Hickey, H. "Household Robots Do Not Protect Users' Security and Privacy, Researchers Say." *UW News* (2009). URL http://www.washington.edu/news/2009/10/08/household-robots-do-not-protect-users-security-and-privacy-researchers-say/.

[9] Zagouras, Panagiotis, Kalloniatis, Christos, and Gritzalis, Stefanos. "Managing User Experience: Usability and Security in a New Era of Software Supremacy." *International Conference on Human Aspects of Information Security, Privacy, and Trust.* Springer, New York City, NY (2017): pp. 174–188.

[10] Bernd, J., Gordo, B., Choi, J., Morgan, B., Henderson, N., Egelman, S., Garcia, D. D., and Friedland, G. "Teaching Privacy: Multimedia Making a Difference." *IEEE MultiMedia* Vol. 1 (2015): pp. 12–19.

[11] Cerrudo, C. and Apa, L. "Hacking Robots before Skynet." *IOActive* (2017). URL https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

[12] Matheny, M. "CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education." CloudPassage (2016). URL https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

[13] Security Magazine. "U.S. Universities Failing in Cybersecurity Education." *Security Magazine* (2016). URL https://www.securitymagazine.com/articles/87062-us-universities-failing-in-cybersecurity-education/.

[14] Bada, M., Sasse, A. M., and Nurse, J. R. (2019). “Cyber Security Awareness Campaigns: Why do they fail to change behavior?” arXiv preprint arXiv:1901.02672.

[15] Kim, E., Jensen, M. B., Poreh, D., and Agogino, A. M. “Novice Designer’s Lack of Awareness to Cybersecurity and Data Vulnerability in New Concept Development of Mobile Sensing Devices.” *Proceedings of the DESIGN 2018 15th International Design Conference*: pp. 2035–2044. Dubrovnik, Croatia, 2018.

[16] Burton, L. H. “An Explicit or Implicit Curriculum: Which Is Better for Young Children?” *The World Congress of the Organization Mondiale Pourl’Education Prescholaire*. Education Resources Information Center, Denmark, Copenhagen (1998).

[17] Selener, D. “Participatory Action Research and Social Change.” No. Ed. 2. The Cornell Participatory Action Research Network, Cornell University, Ithaca, NY. 1997.

[18] Altrichter, H., Kemmis, S., McTaggart, R., and Zuber-Skerritt, O. “The Concept of Action Research.” *The Learning Organization* Vol. 9 No. 3 (2002): pp. 125–131.

[19] TheDesignExchange.org. “TheDesignExchange.” URL https://www.thedesignexchange.org, accessed 02/24/2019.

[20] Crone, M. R., Reijneveld, S. A., Willemsen, M. C., Van Leerdam, F. J. M., Spruijt, R. D., and Sing, R. H. “Prevention of Smoking in Adolescents with Lower Education: A School Based Intervention Study.” *Journal of Epidemiology & Community Health* Vol. 57 No. 9 (2003): pp. 675–680.

[21] Ericsson, I. and Karlsson, M. K. “Motor Skills and School Performance in Children with Daily Physical Education in School–A 9-Year Intervention Study.” *Scandinavian Journal of Medicine & Science in Sports* Vol. 24 No. 2 (2014): pp. 273–278.

[22] Ioannidis, J. P. A. “Why Most Published Research Findings Are False.” *PLoS Med* Vol. 2 No. 8 (2005): e124. https://doi.org/10.1371/journal.pmed.0020124

[23] Runco, M. A. and Jaeger, G. J. “The Standard Definition of Creativity.” *Creativity Research Journal* Vol. 24 No. 1 (2012): pp. 92–96.

[24] Rietzschel, E. F., Nijstad, B. A., and Stroebe, W. “The Selection of Creative Ideas after Individual Idea Generation: Choosing between Creativity and Impact.” *British Journal of Psychology* Vol. 101 No. 1 (2010): pp. 47-68.

[25] Amabile, T. M. “The Social Psychology of Creativity: A Componential Conceptualization.” *Journal of Personality and Social Psychology* Vol. 45 No. 2 (1983): p. 357.

[26] Kudrowitz, B. M., and Wallace, D. “Assessing the Quality of Ideas from Prolific, Early-Stage Product Ideation”. *Journal of Engineering Design* Vol. 24 No. 2 (2013): 120–139.

[27] Kwon, J., and Kudrowitz, B. “Good Idea! Or, Good Presentation? Examining the Effect of Presentation on Perceived Quality of Concepts.” *Artificial Intelligence Engineering Design, Analysis, and Manufacturing* Vol. 32 No. 4 (2018): pp. 380–389.

[28] Yee, Ka-Ping. “Aligning Security and Usability.” *IEEE Security & Privacy* Vol. 2 No. 5 (2004): 48–55.

[29] Johnston, J., Eloff, J. H. P., and Labuschagne, L. “Security and Human Computer Interfaces.” *Computer & Security* Vol. 22 No. 8 (2003): pp. 675–684.

[30] Ibrahim, T., Furnell, S., Papadaki, M., and Clarke, N. “Assessing the Usability of End-User Security Software.” *Proceeding of 7th International Conference in Trust, Privacy, and Security in Digital Business*. Vol 6264: pp. 177–189. Springer, Berlin, Heidelberg, 2010.

[31] Balfanz, D., Durfee, G., Smetters, D.K., and Grinter, R.E. “In Search of Usable Security: Five Lessons from the Field.” *IEEE Security & Privacy* Vol. 2 No. 5 (2004): pp. 19–24.

[32] Cranor, L.F. and Garfinkel, S. “Security and Usability: Designing Secure Systems That People Can Use.” O'Reilly Media, Inc., Sebastopol, CA (2005): pp. 47-74.

[33] Cranor, L.F. and Buchler, N. “Better Together: Usability and Security Go Hand in Hand.” *IEEE Security & Privacy* Vol. 12 No. 6 (2014): pp. 89–93.

[34] Thiese, M. S. “Observational and Interventional Study Design Types: An Overview.” *Biochemia medica* Vol. 24 No. 2 (2014): pp. 199–210.