NIST Internal Report
NIST IR 8558

Report on the Design-A-Thon: Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness

Michael Fagan
Julie Haney
Daniel Eliot
Barbara Cuthill
Kristina Rigopoulos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8558

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8558

Report on the Design-A-Thon: Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness

Michael Fagan
Daniel Eliot
Barbara Cuthill
Kristina Rigopoulos
Applied Cybersecurity Division
Information Technology Laboratory

Julie Haney
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8558

September 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Publication History
Approved by the NIST Editorial Review Board on 2025-07-21

How to Cite this NIST Technical Series Publication
Fagan M, Haney J, Eliot D, Cuthill B, Rigopoulos K (2025) Report on the Design-A-Thon: Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8558. https://doi.org/10.6028/NIST.IR.8558

Author ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Julie Haney: 0000-0002-6017-9693
Daniel Eliot: 0009-0006-3078-555X
Barbara B. Cuthill: 0000-0002-2588-6165
Kristina Rigopoulos: 0000-0001-5223-8801

Contact Information
iotsecurity@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8558/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This report documents the first SOUPS Design-A-Thon, which was held on August 11th, 2024, and focused on Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness. In total, eight individuals participated in the event, forming three teams. The teams each selected a mock product based on a selection of five Product Data Cards developed by the NIST team. Participants used the information on the Product Data Cards to develop a strategy for cybersecurity education and awareness for the product. Teams were successful in planning strategies that utilize novel techniques and sound best practices. From the participant teams' designs, the NIST team identified highlights and takeaways that are further elaborated in this report.

Keywords

cybersecurity; Internet of Things; Design-A-Thon; usability; human factors; education and awareness.

Audience

This report is primarily intended for students and researchers in the fields of IoT cybersecurity and usable security. The topics and discussion of this report may also be useful and interesting to practitioners in these fields, but since the report contains initial findings from a small group exercise, it is not intended as a specific recommendation or guideline for practice.

Table of Contents

List of Figures

Acknowledgments

NIST thanks all the organizers of USENIX SOUPS and the Tutorials and Workshops Co-Chairs, specifically, for the opportunity to bring our idea for a Design-A-Thon to the symposium. We also thank everyone who participated in the Design-A-Thon, giving their time and bringing the great ideas documented in this report.

1. Introduction

On August 11, 2024, National Institute of Standards and Technology (NIST) researchers facilitated a Design-A-Thon titled Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness which was hosted at the 2024 USENIX Symposium on Usable Privacy and Security (SOUPS). The Design-A-Thon was organized by Michael Fagan, Daniel Eliot, Barbara Cuthill, and Julie Haney with support from Kristina Rigopoulos, all members of the NIST Information Technology Lab (ITL). Background on the foundations for this project is provided in Section 2, while details about the planning and execution of the Design-A-Thon are discussed in Section 3.

In total, eight conference attendees participated in the event, forming three teams. Each team selected a mock product based on a selection of five Product Data Cards developed by the NIST team. The Product Data Cards developed for the Design-A-Thon can be seen in Appendix B. Participants used the information on the Product Data Cards to develop a strategy for cybersecurity education and awareness for the product. The team's designs and ideas are documented in Section 4.

Teams were successful in planning strategies that utilize novel techniques and sound best practices. From the participant teams' designs, the NIST team identified highlights and takeaways that are further elaborated in Section 5.

2. Background

2.1. Digital Product Cybersecurity Education and Awareness

The NIST Internet of Things (IoT) Cybersecurity Program has defined an IoT cybersecurity baseline for both technical capabilities and non-technical capabilities. Technical capabilities are those provided by digital products using software and hardware, such as Over-The-Air software update mechanisms or data encryption. Non-technical capabilities are those provided by organizations in support of digital product cybersecurity. Cybersecurity education and awareness is an example of a non-technical cybersecurity capability. The term "education and awareness" is defined as "The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity related information, considerations, features, etc. of the IoT device." [1] There are many ways this capability can be implemented, but some examples include:

- Instructions in a printed user manual.
- How-to and other instructional videos available online.
- In-person training sessions or remote webinars.
- Information delivered via a product's mobile application.

Cybersecurity education and awareness can provide critical support for the cybersecurity of digital products. Notably, the capability can inform and educate users about other cybersecurity capabilities, particularly technical capabilities. For example, cybersecurity education and awareness can guide users on creating strong access control credentials and permissions for products where such features are supported. Other information can be delivered using this capability as well, such as expectations for use of the product and other cybersecurity expectations, which can reduce the possibility of a risk being missed or otherwise unaddressed when the product is deployed.

For more information about cybersecurity education and awareness, please see NIST Internal/Interagency Reports 8259 [2], 8259B [1], 8425 [3], 8425A [4], and NIST Special Publication 800-213A [5].

2.2. Human-Factors Considerations for Cybersecurity

Particular care should be taken with the messaging and presentation of consumer education materials or users may not engage with or understand them. Users are more likely to read or interact with educational materials that are visually appealing or in alternative formats appropriate to the product (e.g., videos) [6]. Further, materials should be written in language that is understandable to a wide range of users, typically written at no more than an 8th grade reading level for adult users. Translations of education materials into common languages spoken across the customer base should be provided, as is the practice for US federal agencies

[7]. Additionally, materials should meet accessibility[1] standards and guidance (e.g., Americans with Disabilities Act (ADA) and Section 508 of the Rehabilitation Act of 1973) to support users with disabilities.

Since many users may not fully understand cybersecurity risks to their IoT products, education materials should clearly communicate the relevance of product cybersecurity features (what the features do and why these are of importance) and what actions are expected of the users (e.g., changing settings or physically safeguarding the product). Instructions for setting cybersecurity preferences should be clear, simple, and achievable for those without cybersecurity expertise. To support diverse users with different cybersecurity and technical needs, skills, and interests, a layered approach for education materials may also be helpful; first present basic information, then provide links to more detail for those who need or want it.

[1] In this report the term "accessibility" is used in the context of limiting or removing barriers for individuals with disabilities to use technology, access information and services, and participate in society generally.

3. Report from the Design-A-Thon

A "Design-A-Thon" is an interactive event where individuals or teams are given a design task to work on within a given timeframe (generally several consecutive hours). It is closely related to the concept and approach of a Hack-A-Thon but isn't as focused on technical solutions or coding. As such, Design-A-Thons can be a useful tool to bring inter-disciplinary thinking with the aim of novel solutions to problems. NIST researchers planned the Design-A-Thon to target cybersecurity education and awareness for digital products. Education and awareness of cybersecurity draws on several disciplines, and the research like that published at SOUPS captures many of the insights and approaches that can help develop effective strategies for educating users and making them aware of cybersecurity related to the digital products they use. The aim of this event was to encourage outside-the-box thinking around this topic and leverage participants' knowledge and expertise to develop ideas and strategies for informing users of the digital products about the areas important to product lifecycle cybersecurity.

3.1. Before the Event

The event webpage was created to provide basic information to potential participants about the event (e.g., goals, objectives, agenda) in the weeks leading up to SOUPS. Additionally, a Call for Participants Flyer was also developed and used to provide additional information about the Design-A-Thon to interested individuals. The Call for Participants was distributed by the SOUPS organizers when promoting the program of workshops accepted to the conference, including the Design-A-Thon. The Call for Participants Flyer can be found in Appendix A of this report.

The NIST team developed a series of Product Data Cards to support the Design-A-Thon. These cards served as the prompts for teams to design approaches for cybersecurity education and awareness related to the products described on the cards. Each of the Product Data Cards featured a mock IoT product and fictional information about the product, its development, and supported cybersecurity. Each card contained the following information:

1. Name of the product and its manufacturer.
2. The target market of the product, what components comprise the product (e.g., mobile app, backend), and where the product is acquired by customers.
3. The features of the product.
4. Information about the product's lifecycle and cybersecurity support throughout the lifecycle.
5. How data is protected and access is controlled.
6. How the product can be configured by customers and other users.
7. How the manufacturer can communicate with customers and other users.

Around these 7 topics, the NIST team created five unique Product Data Cards that teams could choose from as a focus of their designs. The NIST team varied products by multiple aspects such as functions, features, target market to provide distinct starting points for the teams and to

explore how approaches to cybersecurity education and awareness may be similar or different for products and audiences. All Product Data Cards created for this event can be found in Appendix B.

3.2. Event Logistics

This event occurred at the Twentieth Symposium on Usable Privacy and Security held in Philadelphia, Pennsylvania, on Sunday, August 11, 2024. A total of eight participants attended the Design-A-Thon, forming three design teams. Team 1 had three team members, Team 2 had two team members, and Team 3 had three team members. Participants were all college or graduate student attendees of the SOUPS conference. Three NIST team members were present to coordinate and run the event. Design teams mainly worked independently, but the NIST team did provide an introductory presentation (the slides of this presentation are available in Appendix C). This event was organized as follows:

1. The NIST team gave a brief introduction that defined cybersecurity education and awareness and provided other background information for participants as well as instructions for the Design-A-Thon.
2. Each design team selected their target product from the selection of Product Data Cards.
3. Design teams brainstormed ideas and discussed potential approaches before a brief check in with the NIST team after 30 minutes to ensure all teams were making progress.
4. Design teams developed and honed their ideas for about an hour before another brief check-in with the NIST team.
5. Design teams finalized their ideas in the last hour.
6. Each design team presented their plan, including any examples and mock-ups.

Throughout the event, NIST team members were available to answer questions from the teams and captured images, artifacts, and design progression notes. The following section details artifacts from the Design-A-Thon from each of the design teams.

4. Designs

This section describes each design team's plan, as well as images, and other artifacts from the Design-A-Thon.

4.1. Team 1

Team 1 selected the IoT Children's Toy as their product. The team designed around accessibility for both parents and children. For example, they included a storybook-style manual and music-based educational approaches for children. Figure 1 shows the mock-up the team created for the cover of the storybook manual for children.

Fig. 1. Hand-drawn concept of the storybook manual for children.

The team identified that firmware updates are critical to the cybersecurity of a smart teddy bear. Team participants also noted that privacy was also noted as a critical concern. The team envisioned utilizing videos and physical manuals to communicate with customers and users. They developed two manuals: one for parents and another for children, allowing for a more targeted audience approach. The adult manual was detailed and focused on salient tips and direct, easy access to resources. The child manual was designed around the idea that the child could help drive cybersecurity and that the product could help teach good cyber hygiene. For example, the eyes of the bear can glow red when an update is needed, prompting the child to seek help, as the team describes in their mock-up of the story book in Fig. 2.

Fig. 2. Sample pages for the storybook manual for children.

The team also pitched a song that the bear could sing that is about and aimed to create cybersecurity awareness. Figure 3 below shows the draft song the team developed.

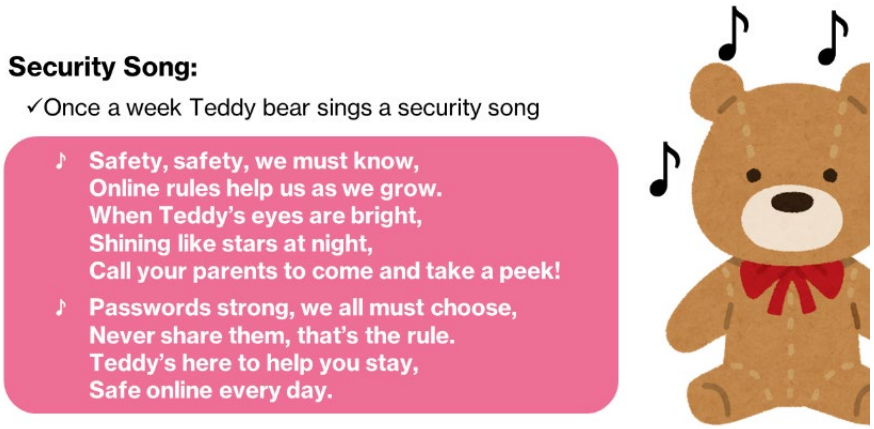


Fig. 3. Cybersecurity-related song created for the toy's cybersecurity education and awareness plan.

4.2. Team 2

Team 2 selected the IoT Security System as their product. They developed an app-based approach that allowed for directed information accessibility for users. The app for the product was identified as the primary portal for cybersecurity education and awareness. In the team's words:

"The SafeCo app should offer an intuitive, easy-to-navigate interface that makes managing your home security simple. It includes a chat system for real-time cybersecurity support, along with quick access to digital manuals and our website for additional resources. Should have a customizable dashboard to stay updated with instant notifications to keep your systems secure."

Fig. 4. Mock-up of how cybersecurity education and awareness information could be delivered via the app.

The team also proposed a digital manual that is sent upon registration. This would include a quick start manual, a single sheet of key information that presents a series of quick start lessons. Links to more information and deeper materials would also be included. Figure 5 shows the team's mock-up for the quick start manual.

Fig. 5. Example of the quick start manual proposed to support the product.

The team also proposed a regular newsletter emailed to proactively engage users that will contain information about cybersecurity. User reports of issues and questions can be used to develop content for the newsletters. The newsletters will contain links to “beginner style” information for system set up and usage. A sample newsletter created by the team is shown in Fig. 6.

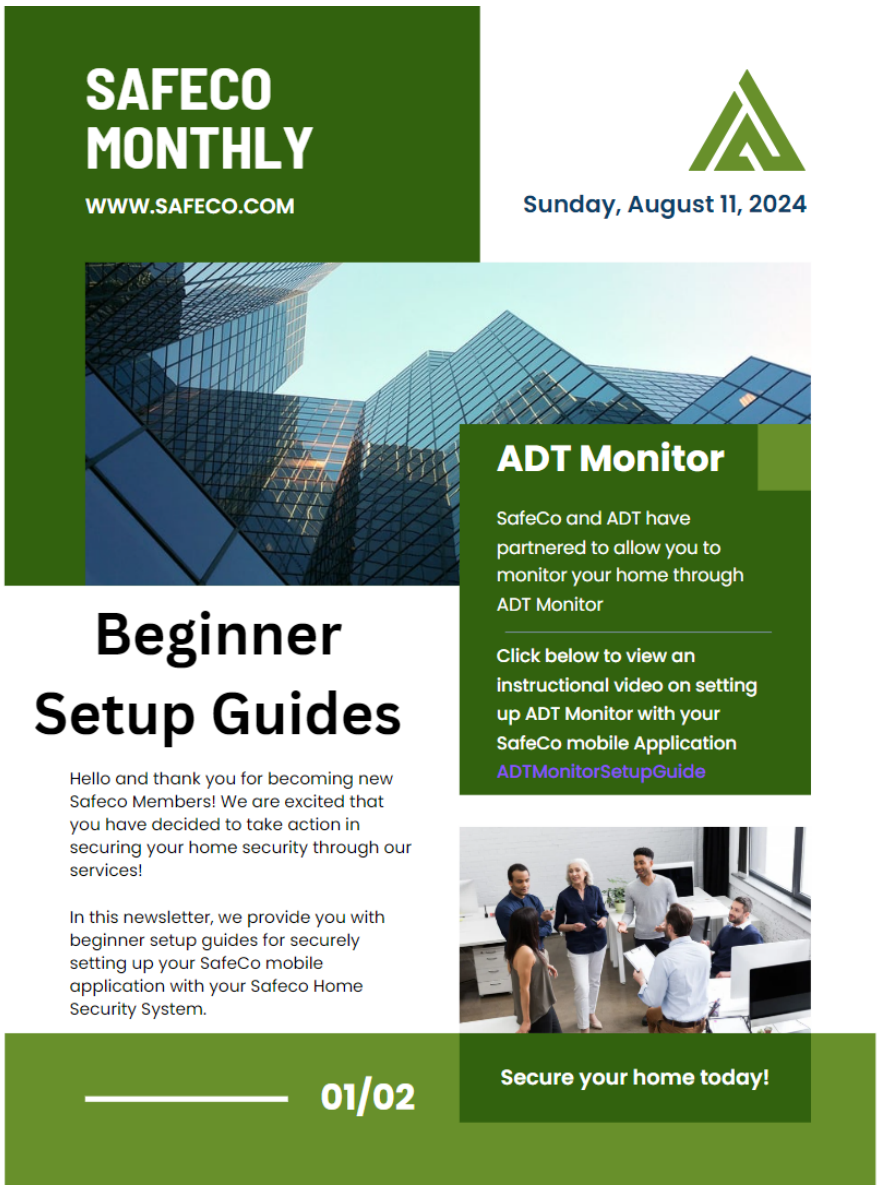


Fig. 6. An example of a cybersecurity-targeted newsletter proposed by the team.

4.3. Team 3

Team 3 selected the IoT Security System as their product. They developed a tailored and gamified approach to delivering cybersecurity education and awareness information. Figure 7 highlights the product's expected users, dimensions, goals, and challenges the team envisioned related to cybersecurity education and awareness for the product. They pointed out two key dimensions to their plan: the various technical skill levels customers may have and how some instances of the product will be managed by "sole operators" while others may be managed by "distributed teams."

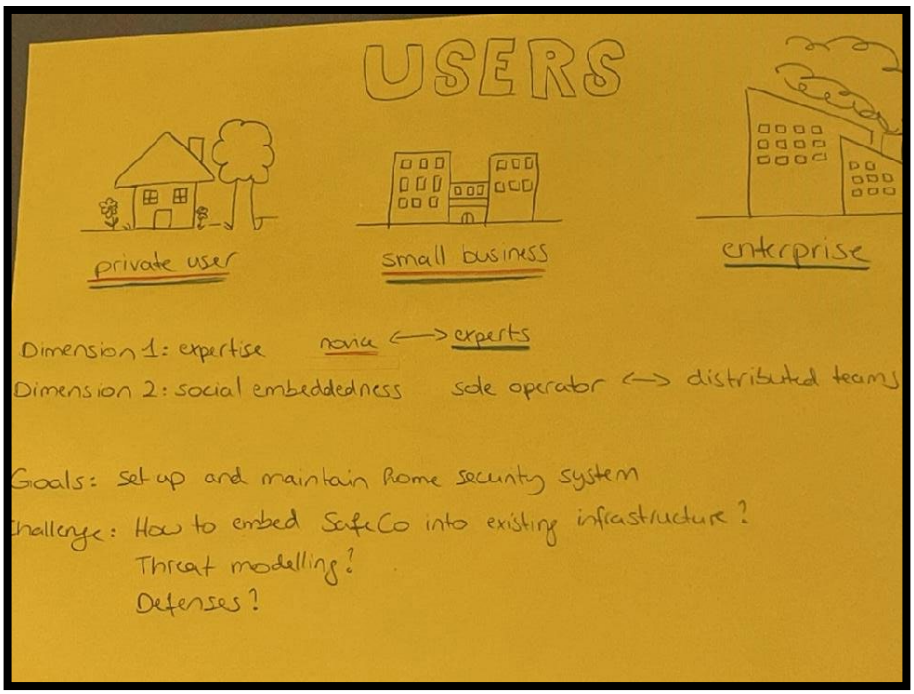


Fig. 7. Planning notes for Team 3's cybersecurity education and awareness strategy.

Based on their two identified key dimensions, the team focused on understanding prospective customers and how they may understand cybersecurity. Figure 8 shows a specific expected user narrative that the team used to target their designs and understand the challenge of different users.

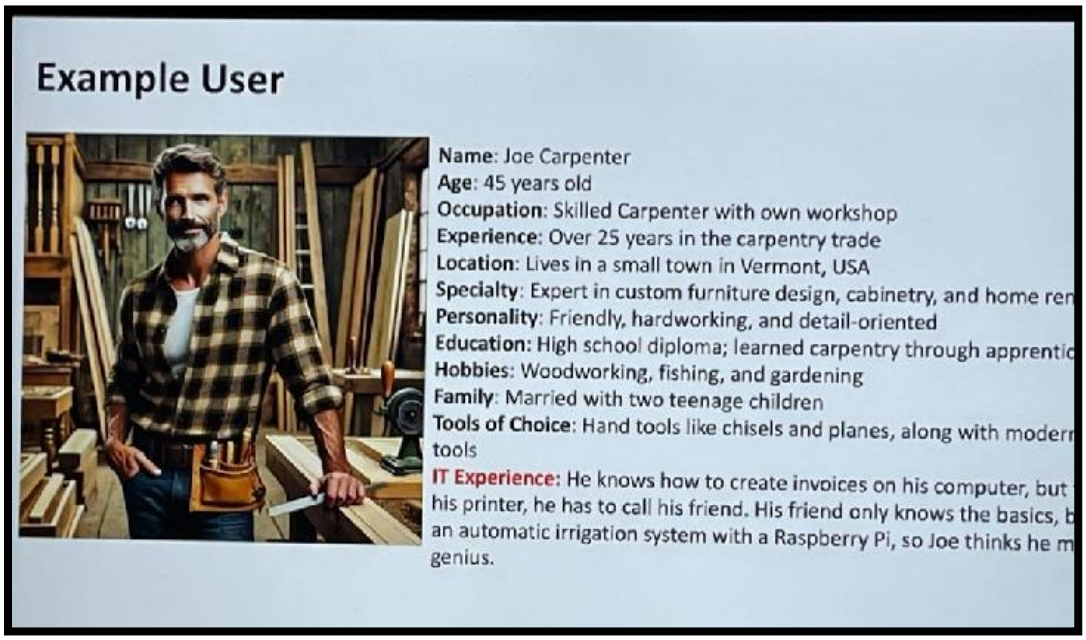


Fig. 8. A detailed user narrative was developed to hone cybersecurity education and awareness approaches. (*Note: cropping of text is due to framing of the source image*)

The planning and narratives culminated in a strategy for cybersecurity education and awareness. The team compartmentalized the key information they hoped to communicate to allow it to be divided and delivered to different users appropriately. They also incorporated guiding and gamification elements to encourage users to engage with and pursue the information. Fig. 9 and Fig. 10 depicts the team's high-level implementation plan.

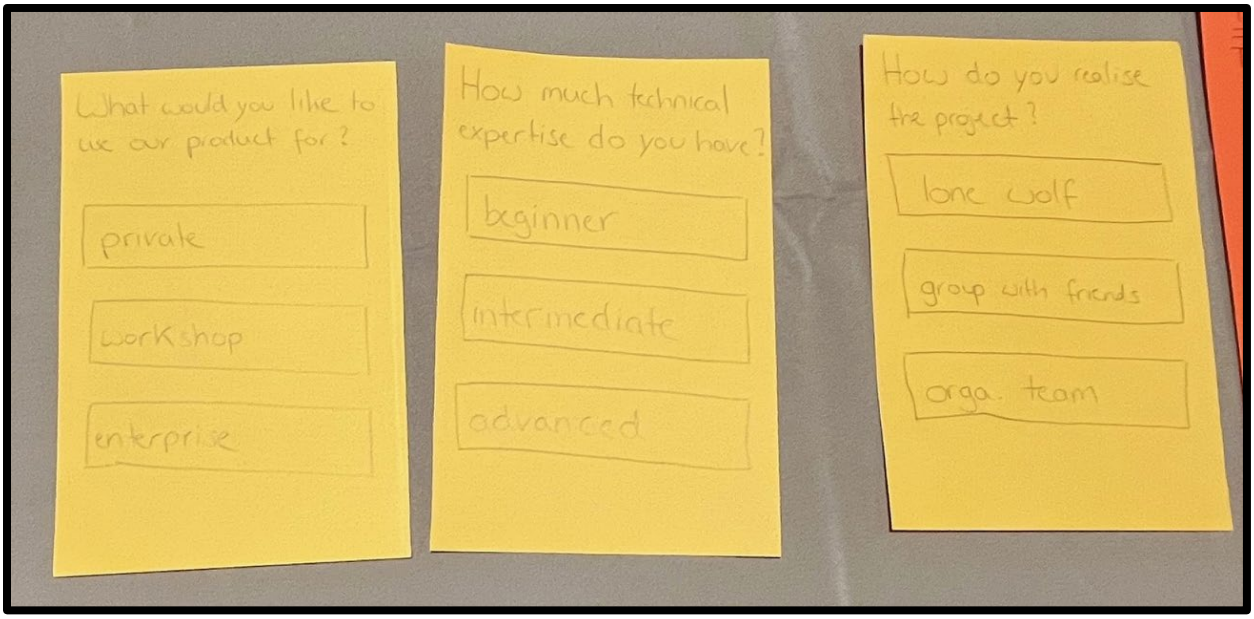


Fig. 9. The team's mock-up of a guided and gamified approach that could be used to support cybersecurity education and awareness.

The three panels in Fig. 9 capture the ideas the team had for a guided approach to delivering cybersecurity education and awareness information based on how the product will be used and by whom. The first panel in the figure asks in what environment the product will be used: personal, workshop, or enterprise. The second panel asks the owner to rate their technical expertise as either beginner, intermediate, or advanced. Finally, the last panel asks whether the product will be used: only by the customer, by them with others, or by multiple users independently. The team proposed that responses to these and similar questions could help guide the customers and other users to the information most pertinent to them.

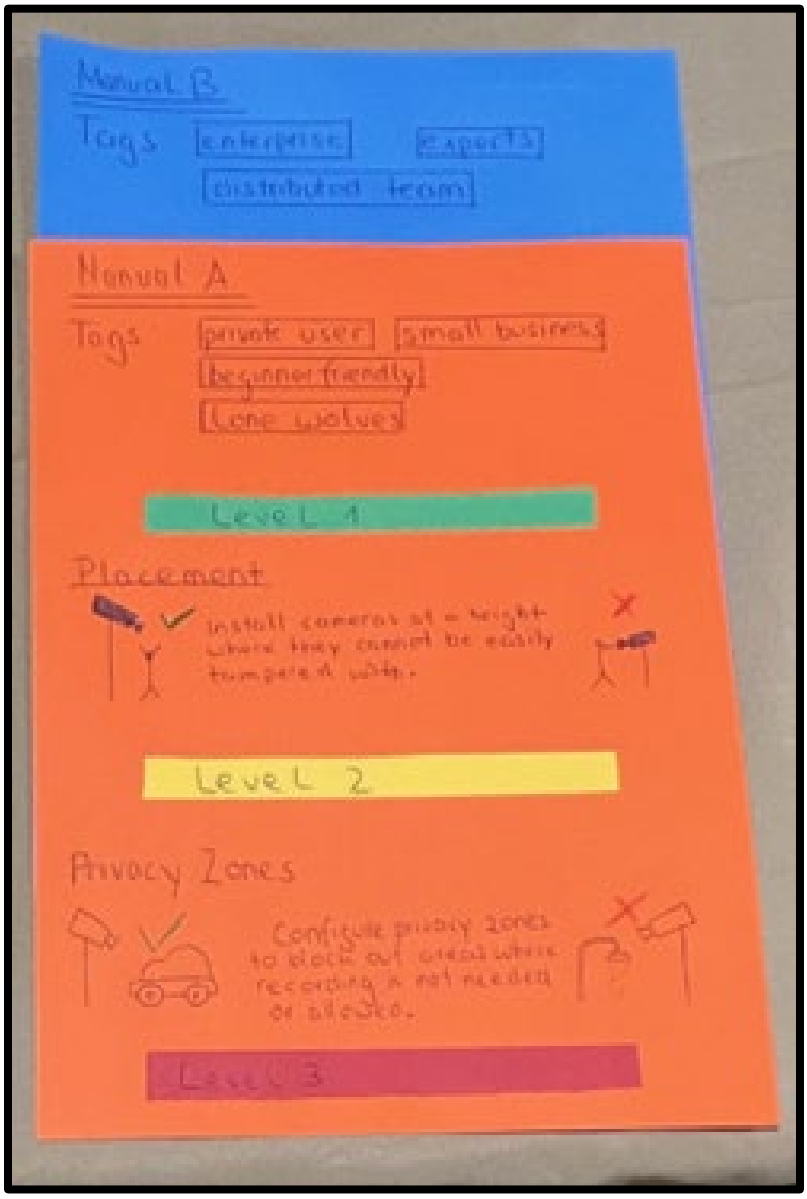


Fig. 10. Mock-up of how answers to the guided questions will impact what customers see and how the content will be gamified.

The team envisioned that the information about customers and users could also be used to tailor the information delivered to customers and how it is gamified, as depicted in Fig. 10. In this context, gamification would be mechanisms that encourage individuals to continue to engage with the content through elements and approaches borrowed from games, such as competition between individuals, feedback on progress, and reward systems for progress. For example, for the IoT security system product, the team proposed organizing cybersecurity education and awareness information into levels, with the lowest level having the most accessible content and higher levels having more information of potentially increasing complexity. Customers and users would be introduced to the lowest level appropriate for them and encouraged to progress to higher levels, thus "leveling up" as in a game.

5. Discussion

This section presents observations and takeaways from the event and teams' designs that were generated after the event and can inform future research and standardization efforts.

All three teams identified different approaches in their plans, showing the wide range of tools and concepts that can be used for cybersecurity education and awareness for IoT products. As teams discussed and identified their plans, they found that standardization of available approaches and selection of appropriate approaches could help increase the speed of material development. All teams deeply considered the expected customers of each product to ensure awareness and education approaches were adequately tailored. Teams indicated that any standardization effort should similarly be human-centric and consider the spectrum of potential users of a given application or product. Unlike some areas of cybersecurity (e.g., encryption) which require limited human interaction, particularly with users, education and awareness addresses the human-in-the-loop and so depends, in large part, on human-factors for efficacy.

All three teams specifically considered how their designs could be "easiest" for users to use, understand, and be most accessible. Teams 1 and 3 incorporated gamification and other interactive elements to encourage users to pursue cybersecurity topics. For example, Team 3 attempted to gamify the pursuit of cybersecurity knowledge relative to the product by building out "levels" of concepts that build upon each other so that users could "level up" at their pace. Understanding and encouraging cybersecurity engagement has been a focus of research for the SOUPS community [8][9][10][11][12][13], and so the teams brought the insights from that research to the practical tasks of the Design-A-Thon.

The contextual nature of cybersecurity education and awareness approaches was apparent when two teams (i.e., Teams 2 and 3) selected the same product but developed different approaches and focused on different aspects of the design. Teams 2 and 3 homed in on different information that may be useful at different times during the product's lifecycle. In one case, Team 2 focused on ensuring information was at users' fingertips, particularly when support was needed. In the other case, Team 3 considered how individuals could be encouraged to engage on cybersecurity education and awareness outside of times they needed support, landing on gamification elements. Research shows that gamification of cybersecurity education and awareness can drive engagement for individuals around the subject [14], but for IoT products, gamification elements should not get in the way when users need support or specific information. In general, the divergence in focus between Teams 2 and 3 highlights the breadth of considerations to be made in designing these solutions, which can be a challenge for manufacturers and others to address when developing a product.

Many roadblocks can exist for manufacturers and other developing approaches for cybersecurity education and awareness related to IoT products, such as not realizing the breadth of variables and aspects to consider, underestimating the time to consider and develop effective solutions, and not knowing or having the ability to implement the most effective solution for all cases. Marketing and other aspects of the product development lifecycle can impact what are the best or most applicable approaches for cybersecurity education and awareness. Products and manufacturers may have access to unique communication channels

that can be useful for cybersecurity communication (e.g., a mobile application). Manufacturers may have a design language or customer interaction approach developed independently of the product, intended to be used by the entire organization that may impact the approach to cybersecurity education and awareness. There may be an opportunity for additional research and future standardization efforts that explore and document these considerations while also linking them with existing and novel approaches for IoT product cybersecurity education and awareness.

Cybersecurity for consumer products could be driven by the upcoming United States Cyber Trust Mark [15], the European Union's Cyber Resilience Act [16], and existing labelling programs such as Singapore's Cyber Security Agency's Cybersecurity Labelling Scheme for IoT [17]. Cybersecurity education and awareness specific to products labelled by these programs and in general as more consumers see these labels may increase the need for future research and standardization that prioritize practical application of concepts and clear, direct guidance for the community.

Our team's primary goal with planning and executing the Design-A-Thon was to explore effective approaches to digital product cybersecurity education and awareness, but the team did have insights that did not fit into this core objective. First, the team observed that the Design-A-Thon proved a useful mechanism to engage the teams on human-centered cybersecurity concepts and may be helpful for a variety of age groups with different educational backgrounds. For example, the Product Data Cards could be adapted for use in middle or high school settings and can be a tool to engage a variety of groups of students on cybersecurity topics (e.g., those interested in cybersecurity, graphic design, or education). A Design-A-Thon may also be useful as a component to a larger project inside and outside of the classroom setting. For example, teams could develop an original product idea over the course of a semester, seeing its design through to the point of devising the cybersecurity education and awareness approaches as our teams did at this event. Since these topics were not the focus of our team's effort, future work could explore these educational possibilities and support educators in their use of Design-A-Thons and similar approaches to teach the next generation of cybersecurity workers.

References

[1] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259B. https://doi.org/10.6028/NIST.IR.8259B

[2] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. https://doi.org/10.6028/NIST.IR.8259

[3] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

[4] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B, Evans C (2024) Recommended Cybersecurity Requirements for Consumer-Grade Router Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425A. https://doi.org/10.6028/NIST.IR.8425A

[5] Fagan MJ, Megas KN, Marron JA, Brady KG, Jr., Cuthill BB, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A

[6] Zhang-Kennedy L and Chiasson S. (2021) "A systematic review of multimedia tools for cybersecurity awareness and education." ACM Computing Surveys (CSUR) 54, no. 1, pp. 1-39. https://dl.acm.org/doi/abs/10.1145/3427920

[7] Plain Writing Act of 2010, Pub. L. No. 111-274, 124 Stat. 2861, 2862 and 2863 (2010) Available at https://www.govinfo.gov/app/details/PLAW-111publ274

[8] Balash DG, Ali MM, Kanich C, and Aviv AJ. (2024) " I would not install an app with this label": Privacy Label Impact on Risk Perception and Willingness to Install {iOS} Apps. (USENIX, Berkeley, CA) Twentieth Symposium on Usable Privacy and Security (SOUPS 2024), pp. 413-432. Available at https://www.usenix.org/system/files/soups2024-balash.pdf

[9] Prange S, Knierim P, Knoll G, Dietz F, De Luca A, and Alt F. (2024) {“I} do (not) need that {Feature!”}–Understanding {Users’} Awareness and Control of Privacy Permissions on Android Smartphones. (USENIX, Berkeley, CA) Twentieth Symposium on Usable Privacy and Security (SOUPS 2024), pp. 453-472. Available at https://www.usenix.org/system/files/soups2024-prange.pdf

[10] Chen X, Doublet S, Sergeeva A, Lenzini G, Koenig V, and Distler V. (2024) What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory. (USENIX, Berkeley, CA) The Twentieth Symposium on Usable Privacy and Security (SOUPS 2024), pp. 487-506. Available at https://www.usenix.org/system/files/soups2024_slides-chen.pdf

[11] Williams O, Choong Y, and Buchanan K. (2024) Youth Understandings of Online Privacy and Security: A Dyadic Study of Children and their Parents. (USENIX, Berkeley, CA) Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), pp. 399-416. Available at https://www.usenix.org/system/files/soups2023-williams.pdf
[12] Usman W, Hu J, Wilson M, and Zappala D. (2024) Distrust of Big Tech and a Desire for Privacy: Understanding the Motivations of People who have Voluntarily Adopted Secure Email. (USENIX, Berkeley, CA) Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), pp. 473-490. Available at https://www.usenix.org/system/files/soups2023-usman.pdf
[13] Huang H, Demetriou S, Hassan M, Tuncay GS, Gunter CA, and Bashir M. (2024) Evaluating User Behavior in Smartphone Security: A Psychometric Perspective. (USENIX, Berkeley, CA) Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), pp. 509-524. Available at https://www.usenix.org/system/files/soups2023-huang.pdf
[14] Gwenhure AK, and Rahayu FS (2024) Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review. (Genoa, IT, Serious Games Society) International Journal of Serious Games, Vol. 11(1), pp. 83-99. Available at https://journal.seriousgamessociety.org/index.php/IJSG/article/download/719/527
[15] Federal Communications Commission (2025) *U.S. Cyber Trust Mark*. Available at: https://www.fcc.gov/CyberTrustMark
[16] European Commission (2025) *Cyber Resilience Act.* Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[17] Cyber Security Agency of Singapore (2025) *About Cybersecurity Labelling Scheme for IoT - CLS(IoT)*. Available at: https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about

Appendix A. Call for Participants

Designing Effective and Accessible Approaches for Digital Product Cybersecurity Education and Awareness

A Design-A-Thon at

The Twentieth Symposium on Usable Privacy and Security (SOUPS)
Philadelphia, PA on August 11, 2024

Abstract: Efforts across the globe have kicked off to drive cybersecurity in digital products. Interest in digital product cybersecurity is welcome, but technical considerations frequently take priority over non-technical measures. Strong cybersecurity capabilities built into digital products can be weakened, circumvented, or ignored if users are not aware of the capabilities or not well-versed in cybersecurity. User education and awareness has been proposed to increase users' knowledge of cybersecurity risks in digital products, communicate their role in securing their products, and empower them to leverage product cybersecurity capabilities. However, education strategies are not well reflected in guidance and standards. **This design-a-thon will explore creating effective and accessible education and awareness of cybersecurity for digital products**, drawing together the decades of research and expertise of the SOUPS community. The event will have teams propose, discuss, compare, and develop ideas and strategies for informing customers and users of digital products about cybersecurity during the products' lifecycle, with a focus on solutions that have potential for long-term standardization. We encourage the community to think outside the box to leverage their knowledge and expertise for approaches to communicating with individuals. After the event, we will bring the findings to cybersecurity standards and guidance development.

Event Description: This design-a-thon will explore creating effective and accessible education and awareness of cybersecurity for digital products, drawing together the decades of research and expertise of the SOUPS community. Teams will develop an education and awareness strategy for example digital products (organizers will provide one product per team) that can inform users about:

- The product's cybersecurity capabilities;
- How to maintain the product during its lifetime and after the period of security support;
- How the product can be securely reprovisioned or disposed of;
- Vulnerability management options that could be leveraged by users; and
- Additional product cybersecurity information users may need to know.

Teams will document their strategies related to an example digital product assigned to each team. Descriptions of these example digital products will also be provided to participants and will include information about the product: what it is, what is does, how it works, who makes it, and cybersecurity capabilities and expectations. Products will vary on features, manufacturer size and type, and target sector or use case. Participants will be encouraged to think outside the box and leverage their knowledge and expertise to develop ideas and strategies for informing users of the digital products about product cybersecurity, as highlighted above. We will then come together to see what we can learn from the designs and experience of the teams during the exercise.

Register for this event by emailing iotsecurity@nist.gov.

More information about this event and how to participate can be found at our event page: https://www.nist.gov/news-events/external-events/soups-2024-design-thon-designing-effective-and-accessible-approaches

Organizers: Michael Fagan, Barbara Cuthill, Julie Haney, and Daniel Eliot, National Institute of Standards and Technology (NIST)

Fig. 10. The Call for Participants used to inform potential attendees about the Design-A-Thon.

Appendix B. Mock Product Data Cards

Fig. 11. Technical and cybersecurity information for a mock fire monitoring system product.

SafeCo®'s Outdoor Home Security System*

Target Market: Homes, small and enterprise businesses

Product Composition: Smart security camera devices, Motion sensor device, Entry sensor devices, Keypad device, Base station device, Backend, Mobile Application

Acquired From: Retail vendors, national and local home security companies, home automation system vendors

Primary Features: This product provides outdoor home security monitoring and alerting based on user input and settings. The base station is a central communication hub between the sensors and the mobile application and can also emit a siren when home entry points are breached. Users can activate the system via the keypad or mobile application. They can also view real-time video and other sensor data in the mobile application. Users have the option of paying for a third-party security monitoring service, which can call the police in the event a home security breach is detected by the security system. The product can share and receive data from other home/office automation IoT products made by SafeCo and other manufacturers that support the product's protocol.

Lifecycle Information: The user or a technician installing the security system can add system components to the network. Users can set software updates to either automatic or manual in which the owner must accept and apply the update in the mobile application. The owner can wipe all data from and reinitialize the devices using the mobile application, allowing the devices to be disposed of or used by a new owner.

Data Protection and Access Control: Data sent between the monitoring devices, base station, keypad, and mobile application and backend are encrypted to protect the data in transit. Access to data stored by the mobile application or backend is controlled so that only the mobile application can access its data in the mobile device environment (i.e., other applications cannot access its data) and only the data owner can access the data related to their security system. Both the mobile application and backend provide the owner with a method to allow other users to access the data associated with the security system. Access to the product is monitored via the mobile application or backend where use of the security system as well as failed and successful attempts to log into the backend are logged.

Configuration Capabilities: Users can configure the security system's schedule, alerts, and activation using the mobile application. Users can configure connection to one Wi-Fi network upon initialization or reinitialization as well as access to and retention of data stored in the backend or mobile application via those components.

How Customers Can Be Reached: Each product ships with a printed user manual. A digital version of the manual is available on the manufacturer's website. The manufacturer also partners with a third-party security monitoring center that can contact owners. Owners will have an account created with a registered email to access the backend and an instance of the mobile application that can receive push notifications.

*Disclaimer: **This is NOT a real product**. This mock-up was created by NIST for the SOUPS 2024 Design-a-Thon.

Fig. 12. Technical and cybersecurity information for a mock home security system product.

SeeClear®'s Smart Portable Wireless Projector*

NEW!

Target Market: Small and enterprise businesses, K-16 school systems, consumer home entertainment.

Product Composition: Smart projector device, Backend, Smartphone Application

Acquired From: Retail vendors, enterprise automation system vendors

Primary Features: This portable smart projector enables high-quality presentations and entertainment by combining cutting-edge video display technologies with the ability to integrate its features with mobile devices, home or work networks, and streaming content services. The projector includes 3GB of memory and 16GB of storage and comes with its own app store. The product pairs with common voice activation services on the market today, enabling consumers to use voice commands to adjust brightness, volume, or turn the projector on and off. The product has built-in Wi-Fi and Bluetooth, enabling consumers to turn their smartphone or laptop into the projector's remote control and mirror their device screens. The device also has USB and HDMI inputs.

Lifecycle Information: The product is added to the network directly by the user. The product's software package enables network managers to set up, manage, and monitor the projector as a managed device. Software updates will require the owner to accept and apply the update in the mobile application. The projector can be restored to factory default settings using the advanced settings in the mobile application. Manufacturer updates are available for 2 years.

Data Protection and Access Control: The product's screen mirroring and wireless presentation capability relies on the network transmitting data from a user's device over the Wi-Fi to a receiver attached to the projector. Data sent from the projector to the mobile application and backend uses enterprise-level AES-128 bit encryption. The device comes with a manufacturer's password. Users can create a unique device password to restrict access. To use the voice text input function and the search function, consumers must consent to provisions allowing third parties to collect and use consumer voice data. The projector can communicate data with network managers, such as: projector power on/off conditions, lamp life, display settings, how many devices are connected to it, and whether the device is currently being used.

Configuration Capabilities: The product can be configured to connect to any Wi-Fi network. Multiple devices can be configured to connect to the projector at the same time. The product comes with standard apps that cannot be removed, and the consumer can add/remove additional apps via the built-in app store to connect to their cloud storage services, organizational productivity tools, favorite streaming services, or gaming platforms.

How Customers Can Be Reached: The product's packaging includes a printed user manual. A digital version of the user's manual can be found on the manufacturer's website. The manufacturer also has a dedicated customer support hotline.

*Disclaimer: **This is NOT a real product**. This mock-up was created by NIST for the SOUPS 2024 Design-a-Thon.

Fig. 13. Technical and cybersecurity information for a mock wireless projector product.

CoolCo®'s Internet-Connected Smart Thermostat*

Target Market: Homes, small and enterprise businesses

Product Composition: Smart thermostat device, Backend, Smartphone Application

Acquired From: Retail vendors, national and local air-conditioning and heating installation and servicing companies, home automation system vendors

Primary Features: This product sends control signals to air-conditioning and heating systems based on user input and settings. Users can set date or time triggers, as well as triggers related to external temperatures ascertained from the internet based on the known location of the product. It also records and displays air-condition and heating system usage data via the mobile application or a web-browser connected to the backend. The product can share and receive data from other home/office automation IoT products made by CoolCo and other manufacturers that support the Connect protocol.

Lifecycle Information: The product is added to the network either directly by the user or by a technician installing an air-conditioning/heating system or a larger home automation system. The thermostat needs the mobile application to send the network information (e.g., SSID). Software updates for the thermostat will require the owner to accept and apply the update in the mobile application. The owner of the thermostat can wipe all data from and reinitialize the device using the mobile application, allowing the device to be disposed of or used by a new owner.

Data Protection and Access Control: Data sent from the thermostat to the mobile application and backend uses encryption to protect the data in transit. Access to data stored by the mobile application or backend is controlled so that only the mobile application can access its data in the mobile device environment (i.e., other applications cannot access its data) and only the data owner can access the data related to their thermostat. Both the mobile application and backend provides the owner with a method to allow other users to access the data associated with the thermostat. Access to the product is monitored via the mobile application or backend where use of the thermostat as well as failed and successful attempts to log into the backend are logged.

Configuration Capabilities: The product can be configured to call for air-conditioning or heating if certain conditions are met. It can be configured to connect to one Wi-Fi network upon initialization or reinitialization. Access to data stored in the backend or mobile application can be configured via those components.

How Customers Can Be Reached: Each product ships with a slip of paper containing basic setup instructions and directs customers to a digital version of a full manual hosted on the manufacturer's website. The manufacturer hosts this and additional support information and tools on a special section of their website. Owners will have an account created with a registered email to access the backend and an instance of the mobile application that can receive push notifications.

*Disclaimer: **This is NOT a real product**. This mock-up was created by NIST for the SOUPS 2024 Design-a-Thon.

Fig. 14. Technical and cybersecurity information for a mock internet-connected thermostat product.

Brighter Play®'s Smart Teddy Bear*

Target Market: Families and children, childcare centers, schools

Product Composition: Smart toy device, Backend, Mobile Application

Acquired From: Retail vendors

Primary Features: This product is a toy for children ages 2-4. It provides audible reminders, for example, when it is time to brush teeth, eat breakfast, or go to bed. The product can also play pre-programmed stories when a button on the right paw is pressed and play songs when the left paw is pressed. Reminders, stories, and songs can be configured by adults on the mobile application.

Lifecycle Information: The product is added to the network directly by the user. The toy needs the mobile application to send the network information (e.g., SSID). Software updates for the product are automatic, with an update completed notification pushed to the mobile app after update installation. Recall and safety notifications are both pushed to the mobile application and sent to the owner's registered email address. The owner of the toy can wipe all data from and reinitialize the device using the mobile application, allowing the device to be disposed of or used by a new owner.

Data Protection and Access Control: Data sent from the toy to the mobile application and backend uses encryption to protect the data in transit. Access to data stored by the mobile application or backend is controlled so that only the mobile application can access its data in the mobile device environment (i.e., other applications cannot access its data) and only the data owner can access the data related to their toy. Both the mobile application and backend provides the owner with a method to allow other users to access the data associated with the toy. Access to the product is monitored via the mobile application or backend where failed and successful attempts to log into the backend are logged.

Configuration Capabilities: Users can configure the toy to set reminders or play selected stories and songs. Users can configure it to connect to one Wi-Fi network upon initialization or reinitialization, including when the toy changes location, as well as access to data stored in the backend or mobile application.

How Customers Can Be Reached: Each product ships with a printed user manual. A digital version of the manual is available on the manufacturer's website. Owners will have an account created with a registered email to access the backend and an instance of the mobile application that can receive push notifications.

*Disclaimer: **This is NOT a real product**. This mock-up was created by NIST for the SOUPS 2024 Design-a-Thon.

Fig. 15. Technical and cybersecurity information for a mock children's toy.

Appendix C. NIST Introductory Presentation Slides

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST developed working definitions for IoT products & devices to support our work

An **IoT product** is an **IoT device** and any additional product components that are **necessary** to using the IoT device **beyond basic operational features**.

NIST IR 8425

An **IoT device** has…

At least one **transducer** for interacting directly with the physical world (e.g., a sensor or actuator)

&

At least one **network interface** for interfacing with the digital world (e.g., Ethernet, Wi-Fi, Bluetooth,…)

NIST IR 8259

The IR 8259 IoT Device definition is utilized in U.S. Public Law 116-207, IoT Cybersecurity Improvement Act of 2020

Background and Overview

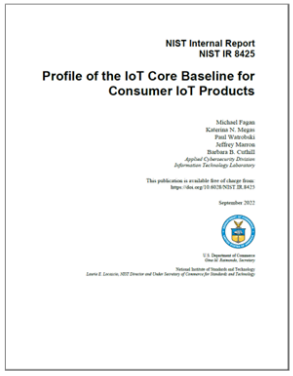
Profile of the IoT Core Baseline for Consumer IoT Products
(September 2022)

- Defines Consumer IoT product scope:

Product Definition

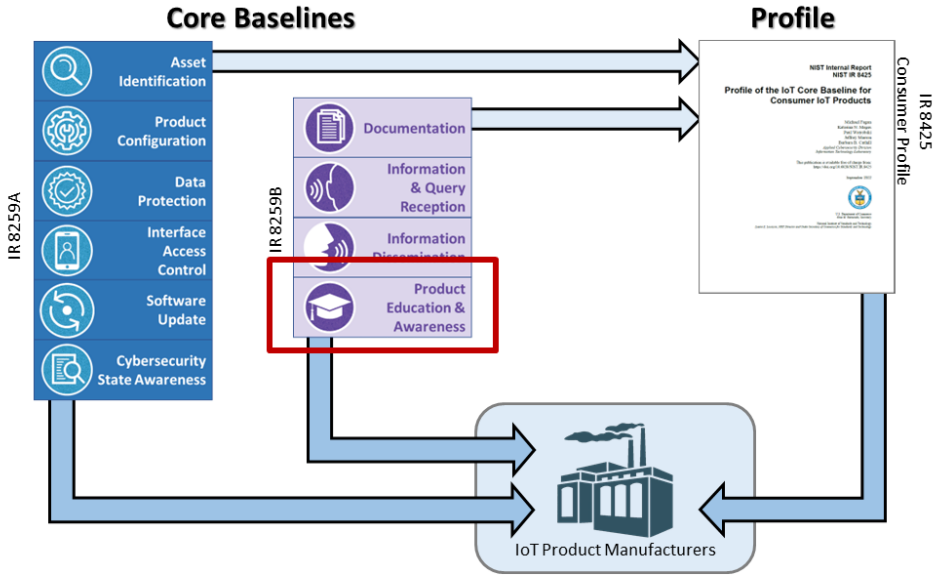
- IoT Device(s), plus any mix of:
- Specialty hardware (e.g., gateway)
- Companion applications (e.g., mobile app)
- Backend support (e.g., cloud services)

- Profiles IR 8259A/B Core Baselines


NIST Internal Report
NIST IR 8425

Profile of the IoT Core Baseline for Consumer IoT Products

Background and Overview



NIST's IoT Cybersecurity Baseline

- Asset Identification
- Product Configuration
- Data Protection
- Interface Access Control
- Software Update
- Cybersecurity State Awareness
- Documentation
- Information & Query Reception
- Information Dissemination
- Product Education & Awareness

NIST IR 8425

Product Education & Awareness

IR 8425: Customers will need to be informed about how to securely use the device to lead to the best cybersecurity outcomes for the customers and the consumer IoT product marketplace.

- Support customers and others in the secure use and safeguarding of IoT devices and associated systems, software, and hardware.
- Supports secure provisioning and on-going cybersecurity report
- Assists customers in dealing with complexities of cybersecurity
- Can help reduce the number of occurrences and related severity of IoT device compromises, thwart attacks against the devices, and reduce the number of vulnerabilities that are exploited and lead to compromised devices.

Product Education & Awareness: Outcome Statement

IR 8425: The IoT product developer creates awareness of and educates customers and others in the IoT product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the IoT product and its product components.

Sub-Outcomes:

1. The IoT product developer creates awareness and provides education targeted at customers about information relevant to cybersecurity of the IoT product and its product components, including product cybersecurity capabilities, maintenance, reprovisioning / disposal, vulnerability management, …

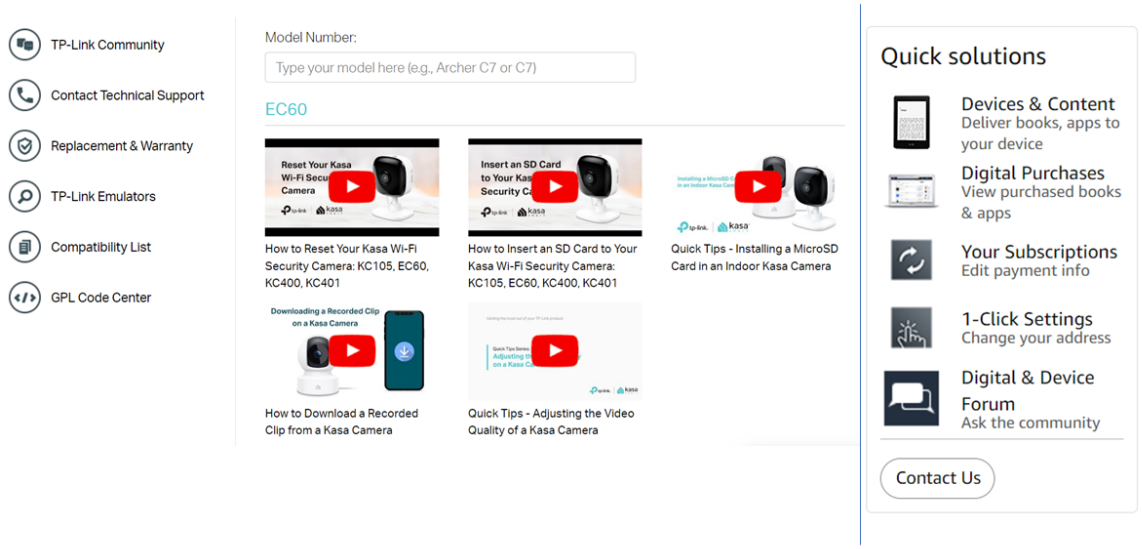
Product Education & Awareness: IR 8259B Background

Education & Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity-related information, considerations, features, etc. of the IoT device.

Common Actions: Educate customers about

1. Presence and use of cybersecurity capabilities
2. Secure reprovisioning / disposal
3. Customer responsibilities
4. Key cybersecurity assumptions and expectations
5. Data backup
6. Vulnerability management options

Examples



Examples

- https://support.google.com/googlenest/answer/9248184?hl=en#zippy=
- https://www.samsung.com/us/about-us/digital-responsibility/cybersecurity/
- https://www.boschsecurity.com/xc/en/support/product-security/

Design Sessions

Develop a plan for cybersecurity education and awareness for your assigned product that can communicate key information to users effective and support their secure use of the product.

Information about the product is provided on your team's Product Data Card. Please feel free to think beyond what is stated about the product!

Brainstorm!

Some guiding questions:

The Product Data Cards provides information about users, but teams should consider other information that may be pertinent such as whether they will create a global plan or one focused on one region or nation.

- Who are the users of the product?
- What cybersecurity information does the user need and when do they need it?
- Are there any aspects of the product that may *complicate* communicating with the user about cybersecurity? Are there any aspects of the product that can *support* communicating with the user about cybersecurity?
- What are methods of communication that could enable successful communication about cybersecurity?

  Feel free to think beyond what is noted on the Product Data Cards and pitch other modes of communication you think might be best for the product or particular information.

Hone Ideas!

Begin organizing your ideas into a cybersecurity education and awareness plan for your product.

Additional brainstorming and new ideas are welcome!

Teams should ensure that they have assembled their ideas into an initial plan for cybersecurity education and awareness by the end of this session.

Time to finalize your education and awareness plans for your product and prepare to present to the group.

You can also execute on your plan! Mock-ups, samples, user narratives, and whatever else you think best communicates your ideas are encouraged and welcomed.