Your security team needs design

KELSEY VAN HAASTER, ThoughtWorks
EMMA LUNDGREN, ThoughtWorks

When rolling out a new security product, engaging the services of an experience designer is not often front of mind. This is a story about why it probably should be, and for us, will be in future.

1. INTRODUCTION

As a designer I've mostly worked on designing software, campaigns or screen flows. I often look at things around me and think that 'this can be better'. Anything from how a shop is laid out to garbage bins and customer support. I believe that anything can and is designed, just by more or less intent. Design has many definitions and one of my favourite ones comes from Jared Spool and is "Design is the intentional rendering of intent" (Spool, 2013) and this "intention" can be applied to anything we see around us. I recently had the chance to put this idea to the test at the software company ThoughtWorks. When I was asked to help with what should have been a simple security problem.

As a security professional, responsible for access and authorisation at ThoughtWorks, I spend a lot of time being very worried. The potential impact of a data breach is unthinkable, organisational reputations built up over decades, can be utterly destroyed in minutes. The most frightening part is that many security incidents are not the result of sophisticated hacking, they happen because someone was in a hurry and simply made a careless mistake.

Password managers are a common solution to this problem, and for various reasons, we assumed they were widely used at ThoughtWorks. However, analysis completed in 2018 challenged these assumptions. This meant that it was imperative to make the idea of using a password manager more attractive to ThoughtWorkers.

This story outlines how a cross skilled team in a couple of weeks used design thinking methods to redesign and implement a new process for rolling out a password manager. As an unexpected bonus the team also changed some mindsets about what design can do and how powerful the design thinking tools can be.

2. BACKGROUND

To start this story, we have to go back a bit in time and first take a look at the world from the perspective of the Identity Team, who are responsible for password security at ThoughtWorks.

The average business user has up to 191 passwords to manage. Approaches like Single Sign On (SSO) (Single Sign On, 2020) can help to reduce this load, but at the same time, having only one password to access multiple resources, increases the criticality of that password being both strong and unique. Many organisations including ThoughtWorks address this by specifying complexity requirements and cycle times for corporate passwords. However, the 2018 National Institute for Standards and Technology (NIST) (Paul A. Grassi) guidelines argue for a different approach (Stocker, 2017). NIST proposes that complexity requirements and short cycle times for passwords should be replaced with greatly increased requirements for password length, much longer, or no cycle times and support for approaches such as diceware to generate passphrases.

Following the release of the 2018 NIST special publication, we were keen to update our password requirements to meet the new guidelines by removing complexity, increasing the minimum password length and reducing cycle time. Since we had always had a policy which provided employees with the ability to reimburse the purchase of a password manager of their choice, we assumed that password manager use was common, and that requiring a much longer password would be no impost.

Kelsey van Haaster, ThoughtWorks, kelseyvh@Thoughtworks.com
Emma Lundgren, ThoughtWorks, elundgre@Thoughtworks.com

We wanted to find out, so we conducted an internal poll in mid 2018 to help us understand the attitude towards password managers in the organisation. The self selected survey, showed a fairly high usage with an 80% uptake in the Americas, Europe and the Asia Pacific, region and a much lower number only 40 to 60% in India and China. The most common reason given for not using password managers is that it's not seen as needed. Other examples of reasons to not use a password manager were usability issues, cost of the software, or that people relied on memory. Yikes! Another problem we uncovered was that although we had a global policy supporting the reimbursement of costs for a password manager, it was not well understood. Further, the policy was inconsistently communicated from region to region, we did not make any recommendations about which product people should purchase, or which expense code should be used, making it difficult to really understand how much we were spending. We were not sending the message we wanted to send to ThoughtWorkers, and this was potentially putting us at risk.

It was clear we needed a different approach. We initiated a conversation with several password manager vendors and it quickly became evident that it would be more cost effective to use our purchasing power to provide all staff and their families with a password manager at no cost and invest our effort in encouraging them to use it. We would simultaneously remove the existing lack of clarity around policy and expense codes and improve the overall security posture of ThoughtWorkers and their families. We spent considerable time developing a set of instructions and communications artefacts, and with great fanfare, we went live.

Our process required people to register with our corporate password manager product, in order to redeem their free product. Almost straight away, many people ran into problems doing this resulting in an avalanche of support tickets taking valuable time away from the Identity Team. Many people unintentionally started using the corporate account which led to licensing issues with the account. One person who did this accidentally and unintentionally shared their passwords in a place where other people in the organisation could access them. Something needed to be done straight away. So the Identity team called for help from our experience design community, thinking that they might help us tweak our communications and instructional artefacts.

3. ENTER THE DESIGNERS

3.1 Human centred security?

To start chipping away at the problems we needed to use a different set of tools and processes than what was usually found in the engineering toolbox. At ThoughtWorks we commonly use design thinking methodologies and human centred design practices for our clients and to solve this problem we decided to use the methods on ourselves. We used the common Double Diamond Framework from the British Design Council (The British Design Council) and the hexagons of Design Thinking by Stanford d.School, (D.School Stanford, 2020) describing the different stages of the design process.

3.2 The full story

To solve this problem we first of all needed a team. A call was given to the organisation and three people put their hands up to help. I was one of the volunteers and together with two more individuals we started. The team had varying experiences with design practices but what they all had in common was:

- **Purpose**. Having a clear reason to work together. This was created by having clear understanding of what the problems were and how this impacted both the business and the customer (in this case the employees of the organisation).
- **Mastery**. Not all of the team members were experts, but we had enough expertise to be able to perform the task at hand.
- **Autonomy**. The ability to decide for themselves how the problem should be solved.

This kind of way to structure teams for motivation is very well articulated by Daniel Pink in his book *Drive*. We used the Design Thinking process as defined by Stanford Design school: **empathise, define, ideate, prototype** and **test** as a framework for our process together with Hypothesis Driven problem solving. These methodologies are not necessarily new, but the purpose of this story is how we made it work in a real-world example.

Throughout the work which lasted about three weeks we followed a few unspoken principles. These principles are all inspired by lean practices which can be found in many places. One is *Lean UX* (Gothelf, 2013) who states that teams need to "focus on the actual experience being designed, rather than deliverables". The second one is *Lean Thinking* (Womack, 2003), where the core idea is to "maximise customer value while minimising waste". I say unspoken because we didn't create these principles together or made them visible in any way. It's when I look back at the work, they become clear. There is no one

place where the following exact principles can be found, however it roughly describes how the team was structured and the core values of how we organised the work.

Focus on root cause. Solve for the true reason for the problem over band-aiding the symptoms.

"Winning the lottery" Documenting is important however only do the amount that supports the case of a team member suddenly leaving because they've "won the lottery". Very often in a consultant world we can at any time get staffed on a client or get pulled into last minute proposals. We were therefore working on the basis of "if one of us wins the lottery" and is out the door the next second. All of our documentation and our process reflected this bare minimum to support decision-making and enough context without creating big reports.

Anyone can do any task, with help from the expert. We aren't limited by who is available or not available.

Go and see. Experience it yourself and feel the pain of your customer is the most valuable insight. Going to where the customer is to watch and listen to them to fully understand their problems was central to what we were doing.

Visualise the work. Make the work we were doing visible to everyone involved at all times.

Remove the unnecessary. Simplify until you can't simplify anymore.

4. OUR APPROACH

4.1 Empathise with the current state

To get as close as we could to what our customer was experiencing, in order to fully understand where the problems and symptoms were located. Only solving the symptoms would possibly make the situation worse so we really needed to understand what our users were going through.

We did an "expert walkthrough" of the existing process with a User Experience Designer making notes of possible points of confusion. We then performed one-on-one interviews with people in Australia, during which we measured the time it took them to finish the setup and any point where they were struggling or needed help.

We visualised all this information in a User Journey map for the different user types. We captured actions they took and any observations the test facilitators were making during the interview. After four interviews we started to see patterns emerging. For example, clicking on links that took people down the wrong path.

4.2 Define the problem space

After having mapped out the user journeys we found we could simplify our five user types down to one with a slight variation. When we moved on to writing problem statements we used the framing question of "What is wrong with what?" and prompts like: "Lack of…" "Not enough…", "Too much…".

At this point we started to "sketch out" problems and plotted them according to what was inside our control and outside our control. This was our "what our circle of concern/influence" actually looked like. This model is used in personal development and wellbeing circles and has for example been used by Franklin Covey in his *7 Habits of Highly Successful People* (Covey, 2011). This model became useful for us to understand our constraints for the problems our users were experiencing. Some root causes were out of our influence for example the vendor existing set up process.

4.3 Ideate on how to solve the problems

We did a quick brainstorming activity on a white board to figure out what small thing we could do to test our hypotheses. We ended up with 5x amount of ideas written as hypotheses statements in the format "We believe that by …. We can solve…. we know this is true when …..". The focus here was to do something small over big changes.

We now felt we had a pretty good handle on the root cause of some of the problems. For example, all of the users we tested experienced a critical failure towards the end of the process that led them down the wrong path, but the reason this was happening was actually because of confusion further up the stream in the flow.

4.4 Prototyping and testing

We tested the ideas in a simple prototype. Avoiding any difficult or complex tools which could allow us to move fast but also to be able to hand over any material to other people which might join our team. Very often in a consultant world we can at any time get staffed on a client or get pulled into last minute proposals. We were therefore working on the basis of "if one of us wins the lottery" and is out the door the next second. All of our documentation and our process reflected this bare minimum to support decision making and enough context without creating big reports.

5. THE RESULTS

Problem 1
The "product" we were designing was a modest instruction. The instruction set we had started with was more like an IKEA instruction set to assemble a really complicated sofa, with multiple levels and a tree house. The seemingly simple process of installing a software program had become so difficult that it required an extensive amount of instructions. The setup process was complicated at best and depending on different factors this process became an impossible mission for most. Factors like what type of history you had with other password managers, which route you had chosen to follow online (email or website), if you were a patient or easily distracted person. If you were lucky you had an expert sitting next to you, guiding you through the process.

Solution 1
The first improvement we made was to reduce the number of instruction sets provided from seven to one.

Problem 2
We noticed that there was one particular part of the flow where everyone was making the same mistake, and the steps didn't fit the mental model of our users. The process would first ask them to set up an account, and then setup another account which was going to be their main account. This resulted in people thinking that they were done after they had set up their first account, leaving them with half a set up done. We thought we could design the flow to fit the mental model of the user rather than the other way around. We also thought that by putting this missed step earlier in the process, less people will miss it because of the distractions and fatigue.

Solution 2
Fit the flow to the mental model of the user rather than the other way around. We put the important step first rather than last.

5.1 Measure of success

The solution was then tracked over a 3-month period and we saw some encouraging results, including, a decrease in critical mistakes for example users putting passwords in the wrong place. We saw reduced time to complete. The first group of people we tested completed (wrongly) the setup in about 40 mins, with the appropriate help from the testing facilitators. This was reduced to an average of 19 minutes—the fastest being done in only seven minutes. There was an increase in sign-ups. This could indicate that more people are using password managers. We now have just under 3000 people using the password manager product, many of whom are first time users of this kind of product. And we saw a reduction in support tickets. This gave more time for the Identity Team to do other more important things.

6. CHALLENGES WE FACED AND HOW WE OVERCAME THEM

Our customers were distributed across the world. We did many of our testing sessions over video call. We were constrained by external providers.

Having to work around an existing complicated procedure by the third party. We identified the constraints and improved the process by improving the things that were in our control. Some of the changes we suggested to the provider were taken into their strategic roadmap of features, but we couldn't rely on them changing so we had to work with that.

Humans being humans. We needed to accommodate instructions to people being distracted, not reading details and making errors.

Adapting to "Winning the lottery" effects. Documenting the minimum amount to get someone else up to speed on a day-by-day basis. The whole design process took longer than expected. There are ways to make the process a bit more efficient. But people who had previously done the setup halfway which when re-launched had to be accommodated for.

7. LESSONS LEARNED

7.1 The Designer's Perspective

This is my first-time coaching and learning from other people through a design process. I've worked almost 10 years in interaction design, and this is the first time I've helped others learn to do design methods, and I've learned more about how to facilitate learning. For example, how to teach others to do user testing.

Being able to let go and have people make mistakes is a good way of teaching. We had an intern on our team and by giving him a sense of purpose and some guidance and amazing things can happen. I learned to start with me facilitating a user testing session with my team members watching and then having that team member do one on their own and to let them make mistakes. The feedback I would give them was much more powerful than having talked through a theoretical session.

Simplicity is hard. Knowing what to strip away and what to keep is an art and a science. Up until the very end we kept asking "do we need it?" and kept removing words and text to keep simplify. Having access to baseline data made this design sprint powerful. I keep confirming my love for one-on-one interviews over surveys. There is a time and place for surveys, and they need to be really well designed to be useful. Writing this article really pushes me to express unconscious knowledge I might have. It has forced me to reflect on the things I take for granted that other people might not.

7.2 The Security Professional's Perspective

We deal with security and security issues all day, every day. What seems obvious to us, is not obvious to everyone. My focus was on getting things technically correct, rather than on getting the outcome I wanted, I had also made a number of assumptions that turned out to be completely incorrect. Even in a technology company, not everyone is technical. People often don't think about security until something goes wrong. Clear communication is much harder than you realise.

Working with the design team on this problem, has helped me to see how they could help us deliver our security message much more effectively, by really understanding things from the end user's perspective. It also reminded me of a key Agile principle, the simplicity and maximising the work not done, is both essential and an art.

8. CONCLUSION

There are still significant amounts of people who don't use a password manager and don't see the benefit of using one. We have put a dent in some of the barriers of password manager usage by making one available through the company and making it easy to sign up but there is still obviously a lot to be done. This small project showed us that by really understanding our user and the limitations we had, we could design a flow that resulted in less mistakes and less support tickets. This project also shows the organisation that customer centric mindsets and processes really work, and we hope to keep challenging the design thinking process in the next challenge: engineering security practices.

REFERENCES

Covey, F. (n.d.). *The 7 Habits of Highly Effective People*. Retrieved from Franklincovey.com: https://www.franklincovey.com/the-7-habits.html

D.School Stanford. (2020). *Get Started With Design Thinking*. Retrieved from https://dschool.stanford.edu/resources/getting-started-with-design-thinking

Gothelf, J. (2013). *Lean UX - Applying Lean Priciples to Improve User Experience.* O'Reilly Media.

Paul A. Grassi, M. E. (n.d.). Digital Identity Guidelines. *NIST Special Publication 800-63-3*. Los Altos, California, USA. Retrieved from NIST.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Single Sign On. (2020, May 20). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Single_sign-on

Spool, J. (2013, December 30). *UIE*. Retrieved from UIE.com: https://articles.uie.com/design_rendering_intent/

Stocker, S. H. (2017, June 5). *Dealing With NIST's about-face on Password Complexity*. Retrieved from Networked World: https://www.networkworld.com/article/3199607/dealing-with-nists-about-face-on-password-complexity.html

The British Design Council. (n.d.). *What is the framework for innovation? Design Council's evolved Double Diamond.* Retrieved from British Design Council: https://www.designcouncil.org.uk/news-opinion/what-framework-innovation-design-councils-evolved-double-diamond

Womack, J. P. (2003). *Lean Thinking.* Free Press.