User-Facing Challenges due to Authorization Policies and Systems in Organizations

Vyshnavi Molakala Narasimhalu (5757991)

May 4, 2023

Word Count - 2530

1 Introduction

Authorization helps organizations protect their crown jewels (assets) and maintain the confidentiality, integrity, and availability of their data, and ensure that only authorized individuals can access the organization's resources [1]. From a user-centred approach, authorization problems in organizations can manifest in a number of ways. One common issue is a lack of access to the resources and information that users need to do their jobs effectively. This can happen when authorization policies are overly restrictive, or when the process for requesting access is cumbersome and time-consuming. Similarly, authorization systems need to be easy to use and understand. A cumbersome authorization system leads to improper use or non-compliance with rules. As organizations adopt more and more technology, it gets difficult to manage access across multiple systems and applications. Users find themselves juggling multiple login credentials and navigating different user interfaces. This can lead to dissatisfaction and missing motivation in users and result in errors, particularly if users are required to switch between multiple systems frequently.

According to S. Parkin, Introduction Lecture about Behaviour and Tasks given at TU Delft, non-secure behaviours are often caused when there is friction between user tasks due to excessive workload and when users are put into a dilemma on which policy to comply with and which to ignore. When it takes a lot of user effort to implement a change in policy, employees may find ways to circumvent the new policy, which can lead to unintended consequences such as security breaches or data loss. Non-secure behaviour and non-compliance are some of the consequences when users put productivity first and security second. However, the challenges of authorization and access control are not confined to drafting efficient policies alone. According to the Compliance Budget model described in [1], to effectively deal with the issues of authorization in an organization, it is crucial to consider the behavioural aspects of users along with designing policies keeping in mind the key principles of usability, productivity, and effort.

This report aims to consider the impact of organizational security and productivity due to the challenges of authorization. The background section gives an overview of the security technology from a user perspective in terms of cost, productivity, and effort (Section 2). The succeeding section includes an intervention design to support the secure behaviour of the user (Section 3). Finally, the report consists of a discussion section on the measures that need to be taken for the intervention to succeed (Section 4).

2 Background

In an organization, the authorization process involves both user-primary tasks and security tasks. The authors of [2] investigate the problems with managing authorization as well as how authorization impedes users' primary tasks. Let's consider some of the user's primary tasks and security tasks.

User primary tasks include:

- Requesting access to resources or information: Users may need to request access to resources or information that they need to complete their daily jobs. This may involve filling out a request form or contacting an administrator for approval.
- Authenticating themselves: Users may need to authenticate themselves before they can access resources or information. This may involve entering a username and password or using a security access token.

[1] https://www.okta.com/identity-101/authorization/

- Navigating access controls: Users may need to navigate access controls in order to access resources or information. This may involve understanding and adhering to different levels of access, such as read-only or full access.

Security tasks include:

- Managing access controls: Security personnel may need to manage access controls, such as setting up new users, revoking access, and monitoring access logs.
- Enforcing policies and procedures: Security personnel may need to enforce policies and procedures related to access and authorization. This may include ensuring that users are following the correct procedures for requesting access and that access is granted only to those who are authorized to access a resource or information.
- Monitoring for security threats: Security personnel may need to monitor for security threats, such as attempted unauthorized access or security breaches.
- Auditing access logs: Security personnel may need to audit access logs to ensure that access is being granted and used in compliance with organizational policies and procedures.

It's important to have a balance between user primary tasks and security tasks while taking into account the user experience, as well as the security risks. This can be achieved by involving users in the authorization process and by keeping the process as simple as possible while still maintaining an adequate level of security.

2.1 The technology, organization, and environment (TOE) framework

TOE framework [3] can be used to analyze the authorization problems in organizations by considering the user costs critical to the success of both security and productivity to achieve user goals in identified contexts.

1. Technology
   The technology aspect refers to the systems and tools used to manage access and authorization in the organization. It can include the hardware, software, and network infrastructure used to implement access controls and authentication mechanisms. One potential problem in this aspect could be outdated or insecure technology, which may make it easier for unauthorized users to bypass access controls or for authorized users to circumvent authorization policies [4]. Users do want to prioritize security, but the existing technologies make it difficult for them to achieve their core objectives. Likewise, Bartsch and Sasse [4] show that even though employees care about security, the rules in place do not comply with their requirements. User costs include the time and effort required to learn and use the technology, the complexity of the system, and the difficulty of troubleshooting and resolving technical issues. These user costs can have a significant impact on productivity, as users may struggle to access the resources and in turn, interfere with their daily tasks.
2. Organization
   The organization aspect refers to the policies, procedures, and governance structures used to manage access and authorization within the organization. A lack of clear policies and procedures for managing access and authorization can lead to confusion and inconsistency in how access is granted and revoked. The authors of [5] talk about shadow security, where employees who are conscious about security and cannot adhere to policies defined by the organization find their own alternatives to these policies. These workarounds are not as secure as officially defined

policies. Herley [6] contends that when the effort ratio is too high, users frequently make rational decisions to overlook security advice. The primary tasks of users are impacted by the time and effort required to request and obtain access to resources, the complexity of the authorization process, and the transparency and fairness of the decision-making process.

3. Environment
   The environmental aspect refers to the external factors that influence access and authorization within the organization. It can include regulatory compliance requirements, industry best practices, and user behaviours and expectations. The authors in [7] conducted interviews with administrators who were responsible to manage authorization and access control policies. They conclude that the non-compliance usually resulted due to information asymmetries, for example, policy authors are different from policy implementers and the access control systems do not have the ability to implement the policies. These factors can result in a lack of alignment between organizational policies and external requirements, which in turn leads to compliance issues or a poor user experience. User costs in this aspect include the effort required to comply with external requirements, the complexity of the compliance process, and the alignment of organizational policies with external requirements. This can have a significant impact on an organization's goals, as they may implement overly restrictive policies that hinder user productivity [8].

By considering all three aspects of the TOE framework, organizations can have a holistic view of the authorization problems and identify potential solutions that address the underlying issues.

3 Intervention

To balance the user costs with the need for security and productivity, the organization must identify the specific contexts in which the authorization problem is occurring and the user goals that are being impacted. By understanding these dependencies, the organization can then focus on specific behaviour elements that need to be addressed in order to solve the problem. For example, if the problem is related to a lack of integration between different systems and applications, the organization may need to focus on investing in Single Sign-On solutions. If the problem is related to a lack of clear roles and responsibilities, the organization may need to focus on creating a clear governance structure for managing access and authorization. Persuasive design, as proposed by Dr. BJ Fogg [9], is a method of design that aims to influence behaviour by making a task easy, attractive, and social. The Fogg Behavior Model (FBM) is a framework that helps to understand how behaviour change happens by identifying the three elements that must be present for a behaviour to occur: motivation, ability, and a trigger. To minimize authorization problems in organizations using persuasive design, we could design an intervention that addresses each of these elements:

1. Motivation
   Clearly communicate the importance of compliance with authorization policies to users. To increase employees' motivation, organizations can create a campaign that emphasizes the importance of authorization in protecting the organization's assets and ensuring compliance with regulations. This campaign can include messages that highlight the consequences of not obtaining authorization (fear appeals), such as data breaches or regulatory fines. It can also highlight the benefits of obtaining authorization, such as increased security and compliance, which can lead to a more positive reputation for the organization. Users can be involved in the policy development process to ensure that their needs and perspectives are taken into account. This can help to increase buy-in and understanding of the policies. Users can further be motivated to comply with the policies and procedures when they are provided with incentives and rewards such as access to additional resources or recognition [10].

2. Ability
   To increase users' ability to comply with authorization policies, the designers should focus on building user-centred authorization systems by simplifying the process as much as possible. The process could be broken down into simple steps, with clear instructions provided at each step. In this process, interviews, surveys, and usability testing need to be conducted to gain insight into how users interact with the current authorization system and how it affects their work. The data collected from user research can be used to identify pain points in the current system. This may include issues such as difficulty in accessing resources, frustration with multiple login credentials, or confusion about the authorization process. Training and support must be provided to users to help them understand and use the new system. This may include providing training on how to request access, how to authenticate themselves, and how to navigate access controls and can also provide online resources, such as FAQs or instructional videos, that employees can access to help them understand the process.

3. Trigger
   Triggers are external cues that remind a person to perform a certain behaviour. In the context of authorization problems in organizations, triggers can be used to remind users to comply with policies and procedures related to access control and authentication. If users i.e., employees find no opportunity or trigger to follow secure behaviour, motivation and ability fade away [S. Parkin lecture about Behaviour Change]. One approach to using triggers is to implement in-app notifications or pop-ups that remind users of the policies and the importance of compliance when they are trying to access a resource. For example, a pop-up message could remind a user to authenticate themselves before accessing sensitive data. This approach can be particularly effective when the trigger is closely tied to the behaviour that is being prompted. Another approach is to use email reminders or push notifications to remind users of the policies and the importance of compliance at regular intervals. For example, an organization could send a weekly reminder to users to update their passwords or review their access permissions. In addition, organizations can use access controls to limit access to resources until compliance with the policies is confirmed. For example, denying access to sensitive data or resources until compliance is confirmed.

By addressing all three elements of the FBM, we can design an intervention that increases the likelihood of employees obtaining authorization. This can help to minimize authorization problems in the organization by ensuring that employees are following the proper protocols and that the organization is in compliance with regulations. Additionally, by making the process easy and accessible, employees are more likely to comply with the process, which in turn will minimize the problems related to authorization.

4 Deployment

Maintaining an intervention for authorization problems in organizations requires ongoing monitoring and evaluation to ensure its effectiveness over time. Additionally, it may be necessary to involve a variety of stakeholders, including security experts, IT personnel, and users themselves, to ensure that the intervention is tailored to the specific needs of the organization. The following steps can be taken to ensure that the intervention is successful over time:

1. Continuously monitor and evaluate the intervention: The management department would be responsible for promoting the intervention and ensuring that employees understand the importance of following proper procedures. They need to regularly monitor and evaluate the intervention by tracking key performance indicators (KPIs) and gathering feedback from users. This will help to identify areas that need improvement and make adjustments as necessary.

2. Keep up with the changing environment: IT personnel must stay aware of changes in the organization's environment, such as new technologies, regulatory changes, and user behaviour because the environment has the ability to undo the success of the intervention [11]. This will help to identify new challenges and opportunities related to authorization.

3. Continuously educate and train users: The HR department would be responsible for continuously educating and training users on the policies, best practices, and new developments. This will help to ensure that users understand the policies and are able to comply with them. Awareness programs through training and education are only the first step in the security of organizations[2]. It is particularly important for employees to apply the knowledge gained through these awareness programs.

4. Regularly review and update the policies: Policy authors and security experts must regularly review and update the policies to ensure they are aligned with the organization's objectives and the user's needs. This will help to ensure that the policies remain relevant and effective.

5. Keep communication open: Keep communication open with users, stakeholders, and IT teams to ensure that everyone is aware of the policies and the importance of compliance.

Overall, the key to maintaining an intervention for authorization problems in organizations is to be proactive and adaptable. This means staying informed about the latest security trends and best practices, as well as being willing to make changes as needed to ensure the intervention remains effective over time. If the intervention is successful, over time it would lead to a decline in authorization problems within the organization. This would be reflected in an increase in the number of employees following proper login procedures and a decrease in the number of incidents related to unauthorized access. As a result, there will be a decrease in security incidents like illegal access to the company's data and systems. We also anticipate a decline in employee dissatisfaction and an uptick in general satisfaction with the authorization process as the intervention is deployed and regularly assessed and modified.

[2]https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf

References

[1] Beautement, A., Sasse, M. A., and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 workshop on new security paradigms, NSPW '08 (pp. 47–58). New York, NY, USA: ACM. doi:10.1145/1595676.1595684

[2] Beautement, A., Sasse, M. A., and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 workshop on new security paradigms, NSPW '08 (pp. 47–58). New York, NY, USA: ACM. doi:10.1145/1595676.1595684

[3] Tornatzky, L. G., Fleischer, M., Chakrabarti, A. K. (1990). Processes of technological innovation. Lexington books.

[4] Bartsch, S., Sasse, M. A. (2012). How users bypass access control and why: the impact of authorization problems on individuals and the organization.

[5] Kirlappos, I., Parkin, S., Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.

[6] Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. NSPW '09 (pp. 133–144). New York, NY, USA: ACM. doi:10.1145/1719030.1719050

[7] Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., Vaniea, K. (2009, April). Real life challenges in access-control management. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 899-908).

[8] Klenow, P. J., Rodriguez-Clare, A. (1997). The neoclassical revival in growth economics: Has it gone too far?. NBER macroeconomics annual, 12, 73-103.

[9] Fogg, B. J. (2009, April). A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology (pp. 1-7).

[10] Wash, R., MacKie-Mason, J. K. (2007, August). Security when people matter: Structuring incentives for user behavior. In Proceedings of the ninth international conference on Electronic commerce (pp. 7-14).

[11] Osman, M., McLachlan, S., Fenton, N., Neil, M., Löfstedt, R., Meder, B. (2020). Learning from behavioural changes that fail. Trends in Cognitive Sciences, 24(12), 969-980.