Hidden Cost of Multi-Factor Authentication

In identity access, cybersecurity confidence is a priority. Reliable onboarding and multi-factor authentication help in reducing security risks. Unfortunately, these come at a substantial cost – authentication fatigue, reduced productivity and unanticipated downtime.

Peig

Time wasted authenticating

Both start-ups and enterprises rely on SSO and MFA to secure employee access. This typically involves entering a username, a 12-character password and using a second factor device for confirmation.

Time lost

10 seconds	Time required to enter a **username and a 12-character password.**
18 seconds	Average time required to authenticate with **commonly used MFA methods** in enterprise identity access - OTP, push notification, or a hardware token.[1]
5 authentications a day	Employees use four to five applications in a typical work day[2] and are **required to authenticate each application once a day.**

5 AUTHENTICATIONS	X	**252** WORKDAYS	X	**28** SECONDS	=	**9,8** HOURS

Even in ideal conditions, implementing MFA will result in **each employee spending an average of 9,8 hours a year** simply logging into their work applications.

28 SECONDS

Multi-factor authentication takes 28 seconds in an ideal situation. There are many other factors that can further reduce MFA efficacy such as an employee's technical capabilities, connection speeds, loading times, or hardware.

CASE STUDY: 2 WEEKS AUTHENTICATING[1]

- 35% users didn't have their MFA device immediately available when needed.
- 66% users had time-out issues with verification code.

Financial loss

The time costs of most MFAs can be translated into an average financial cost of **$303,4 per employee per year**. Per every 100 employees, **enterprises spend $30.340** in direct authentication time.

9,8	X	$30,96	=	$303,4	$30.340
HOURS		AVG. HR SALARY[3]		SINGLE EXPENSE	ENTERPRISE EXPENSE

AUTHENTICATION DILEMMA

Rising cyberthreats require strengthening security measures. In identity access, this often means increasing user authentication frequency.

Unwanted side effects of authentication fatigue

2FA authentication doesn't just have time costs. Requiring employees to go through an authentication process interrupts the tasks they were performing and distracts them from their work. According to a study of external stimuli on productivity[4], it takes people on average **23 minutes to resume an interrupted task** and based on a study of employee authentication in a US governmental organisation[5], task-switching has a 'ripple effect' on focus, concentration and efficacy, not just on the next task, but **all tasks performed for the next 20 to 30 minutes.**

In a typical workday every employee will experience 5 significant authentication distractions. **Each authentication interruption leads to additional 20 minutes of decreased focus, concentration and efficacy.**

5 AUTHENTICATIONS	X	252 WORKDAYS	X	20 MINUTES	=	52 DAYS

52.5 days makes up for 20%! of an employee's average number of workdays per year. MFA requests negatively affect 1/5 of every employee's work year.

Other significant impacts of MFA authentication distraction

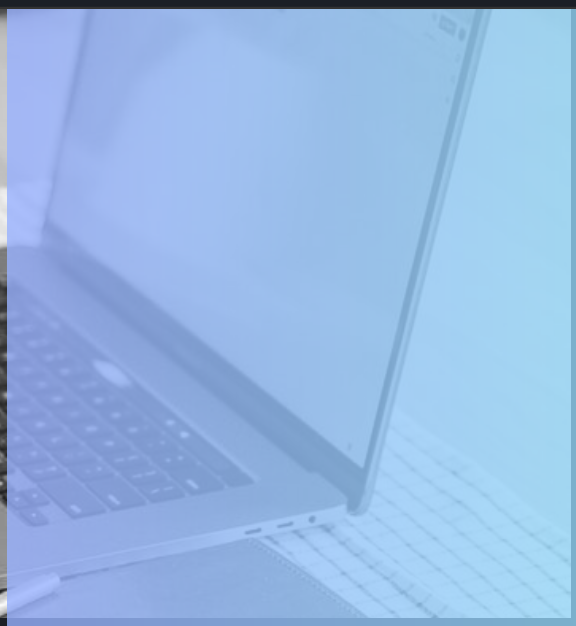
Authentication tasks not only carry significant workload, but also don't contribute to a company's operations and disrupts primary tasks, which reduces productivity and frustrates employees.[6]

Some of the **commonly cited frustrations caused by MFA** are:

- Needing to **re-authenticate**, e.g., after a timeout.
- Having to **manage a large number of credentials** for different systems.
- Constantly needing to **change passwords** for different applications.
- Logging into **infrequently used systems.**
- Struggling with **authentication apps and hardware tokens.**
- Spending **more time authenticating than actually using the application.**

While a company is often more invested in security, employees are usually more invested in productivity. To make up for the productivity loss caused by MFA, **employees tend to adopt coping strategies**, including the use of tools, or reorganizing their work processes to avoid authentication. This avoidance often results in **employees logging in less frequently or completely avoid using certain devices and services**. Many employees also reported **not pursuing innovative ideas because they would have to deal with "security"**.

MFA implementation is intended to increase a company's cyber security but may result in employees not following company policies and procedures and actively avoiding using security solutions, which actually causes a net decrease in overall cyber security.



Extra cost of identity recovery

When an employee forgets a password, or their second-factor device gets lost, broken, or stolen - **a single password reset, or an identity recovery costs on average $70**.[7]

To avoid help desk password resets, some security vendors offer self-service recovery processes. Unfortunately, **in cases of a lost, broken, or stolen authentication device**, an employee will still have to contact a help desk or support center. People lose their phones on average once a year [8], which results in an extra $70 cost per employee each year caused by second-factor device recovery.

The ultimate cost of MFA

Implementing MFA results in far more than just implementation and maintenance costs. Organizations that deploy MFA security are, on average, losing $303,4 just in authentication time and an additional $70 from identity recovery for an aggregate cost of $370,4 per employee per year.

A business with 100 employees would be wasting $37 040 per year by adopting MFA. On top of the hidden financial costs, MFA also negatively affects 20% of employees' productive time!

Taking these hidden costs and impacts into account, despite MFA being considered an economical and convenient security upgrade, current commonly used MFA solutions are neither cost-effective nor efficient.

REFERENCES

1) Second factor authentication time: https://www.usenix.org/system/files/soups2019-reese.pdf

2) Authentication frequency: https://www.pcmag.com/news/the-average-worker-uses-4-to-5-programs-a-day-working-from-home

3) Average US hourly salary: https://www.statista.com/statistics/215630/hourly-earnings-of-all-employees-in-the-us-by-month/ Distraction related productivity loss:

4) https://www.researchgate.net/publication/300918076_Focused_Aroused_but_so_Distractible

5) https://discovery.ucl.ac.uk/id/eprint/1434817/1/The_Great_Authentication_Fatigue_Sasse_Krol.pdf

6) Authentication impact on employees: https://www.researchgate.net/publication/295856246_The_Great_Authentication_Fatigue_-_And_How_to_Overcome_It

7) Cost of password resets / lost authentication devices: Forrester Research, Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers, 2018

8) Average smartphones lost per year: https://www.hongkiat.com/blog/world-of-lost-smartphones-infographic/