

How do you want to use risk-based authentication for login attempts that are classified as low, medium and high risk?

You can use risk-based authentication to increase protection against login attempts that are considered to be at higher risk, such as login attempts from an unknown location or device. [Learn more about risk-based authentication.](#)

	Allow	Optional MFA	Require MFA	Block	Notify users
Low risk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Medium risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
High risk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

RUHR
UNIVERSITÄT
BOCHUM

RUB

Max Planck Institute
for Security and Privacy



Leibniz
Universität
Hannover



“As soon as it’s a risk, I want to require MFA”: How Administrators Configure Risk-based Authentication

[Philipp Markert](#), Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth

August 7–9, 2022 | 18th Symposium on Usable Privacy and Security | Boston, Massachusetts, USA

Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.



Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.



Risk-based Authentication (RBA)

During the login of a user, calculate a risk based on contextual factors like the device and location.



Configuration of RBA

Behavior



Allow



Optional MFA



Required MFA



Block

Notify User



Notify



Don't Notify

Change Notification



Change

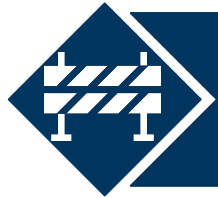


Don't Change

Research Questions



How do administrators configure RBA?



Which obstacles and misunderstandings do they encounter?



What is the impact of previous exposure to other RBA systems and how do different requirements influence administrators?

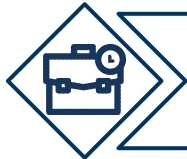
Method



“You are the system administrator of the MediaShop Corporation, where you administrate the online shop dresscode.com”



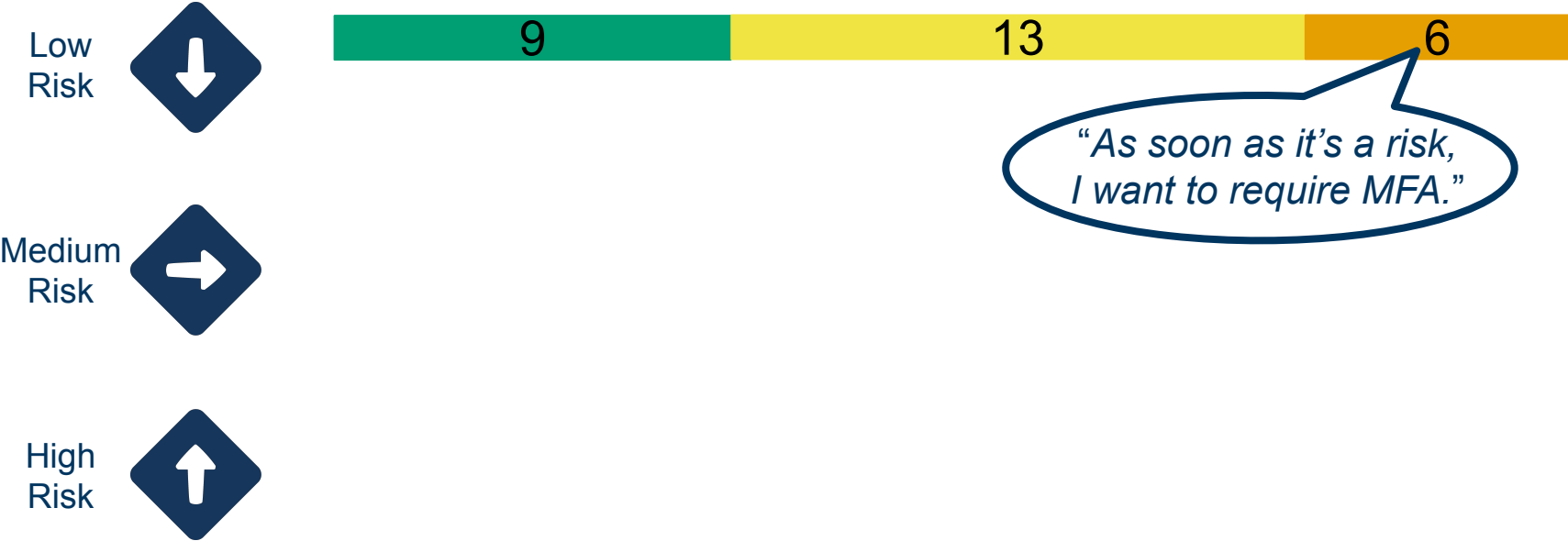
Conducted with $n=28$ participants who work as administrators



10 participants 11–15 years of experience
9 participants >15 years of experience

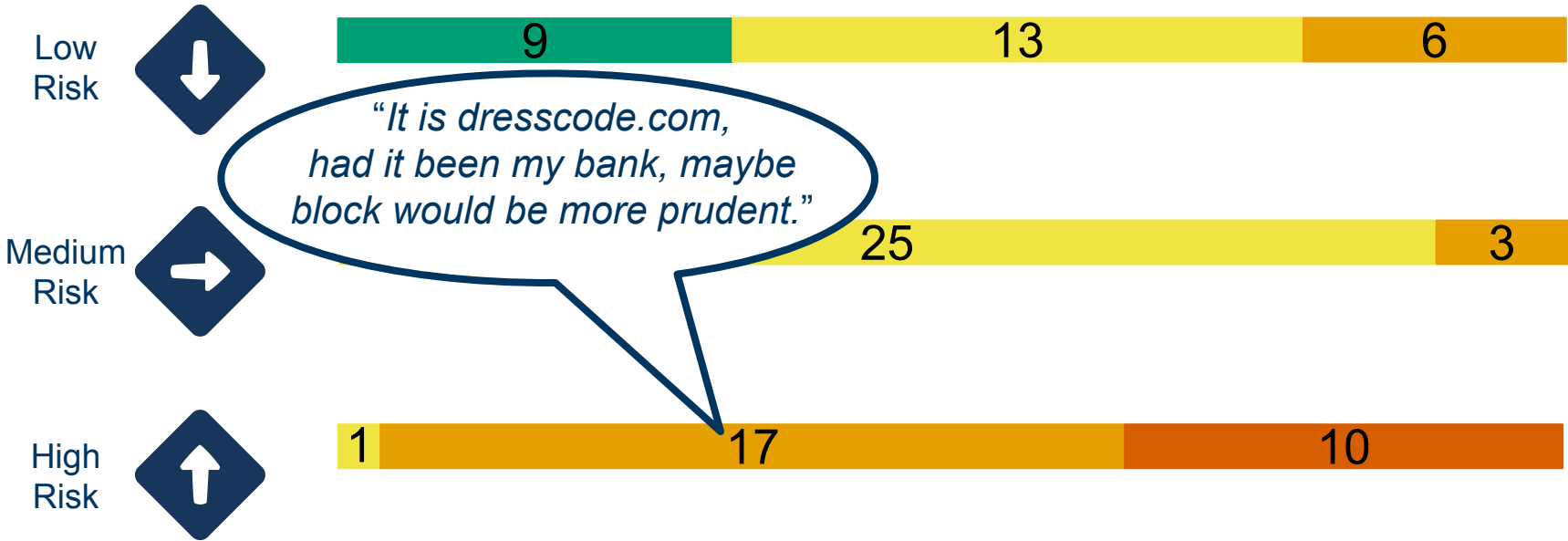
RQ1: How Do Administrators Configure RBA?

Behavior:  Allow  Optional MFA  Required MFA  Block



RQ1: How Do Administrators Configure RBA?

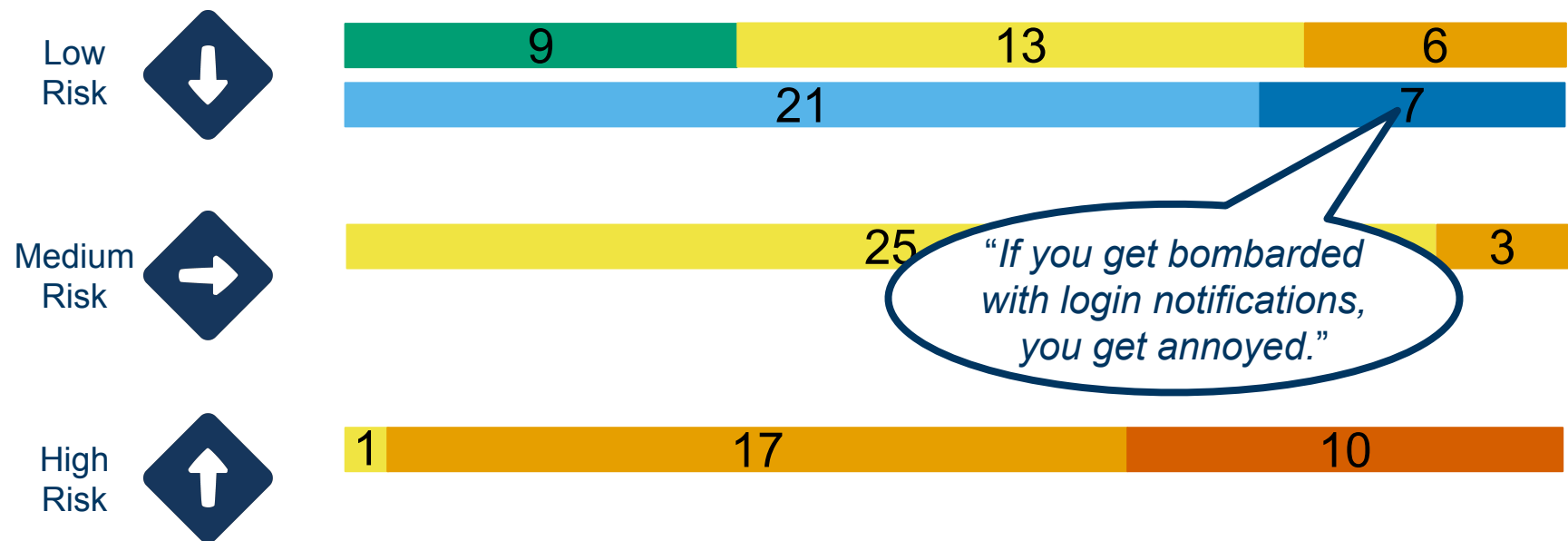
Behavior:  Allow  Optional MFA  Required MFA  Block



RQ1: How Do Administrators Configure RBA?

Behavior: ✓ Allow ? Optional MFA ! Required MFA — Block

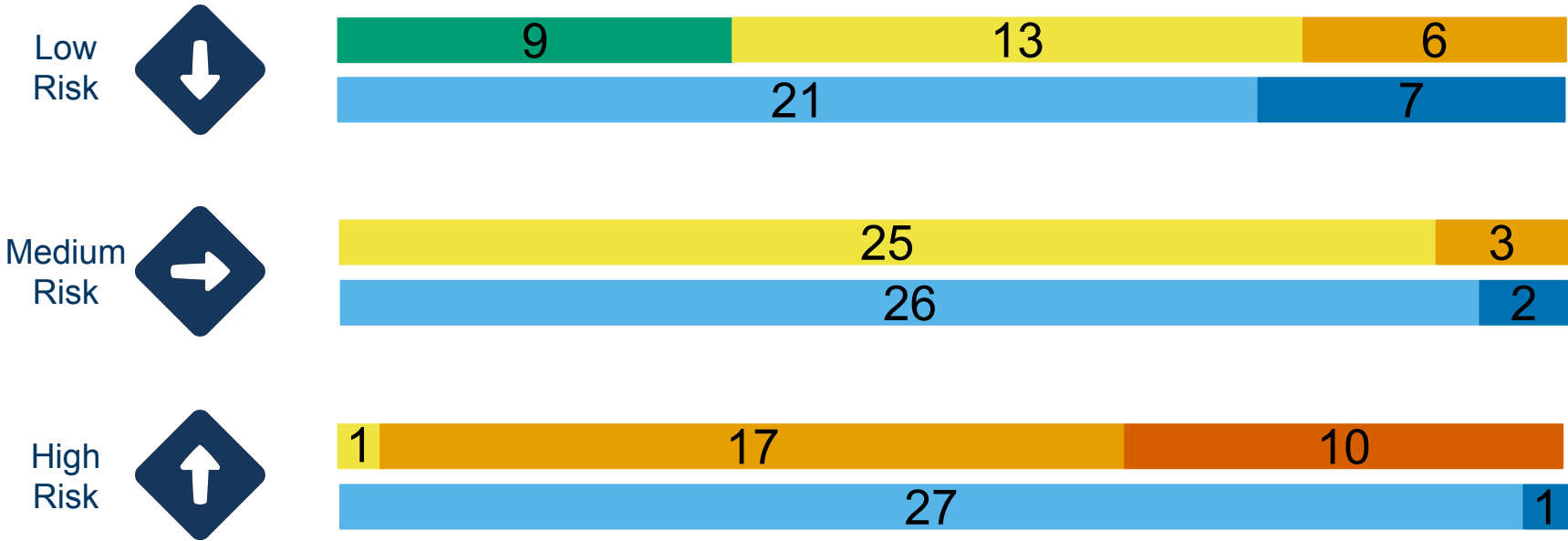
Notification: 🔔 Notify 🔕 Do Not Notify



RQ1: How Do Administrators Configure RBA?

Behavior: ✓ Allow ? Optional MFA ! Required MFA — Block

Notification: 🔔 Notify 🔕 Do Not Notify



RQ2: Which Obstacles and Misunderstandings Do Administrators Encounter?

Understanding Of Risk Level Calculation

“If I don't know exactly what ‘low’, ‘medium’, or ‘high risk’ means, then there is no reason for me to distinguish between them.”

Consequence: User Burdening

“Which parameters classify ‘low’, ‘medium’, and ‘high risk’? That would definitely be a criteria for me when adopting it.”

Consequence: Reduced Sales

Awareness About All Risk Levels



High Risk



Medium Risk



Low Risk



No Risk

Understanding Of Crucial Terms



Optional MFA

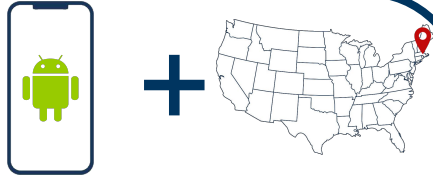
“An attacker will just skip it [...] for users it's convenient to just skip it.”



Block

*“How long will the block last for?
Is this an indefinite block?
Is this just a slowdown of the login attempts?”*

Risk-based Authentication



Risk Levels



Behavior



Notify User



Method



“you’re responsible for the web shop dresscode.com”



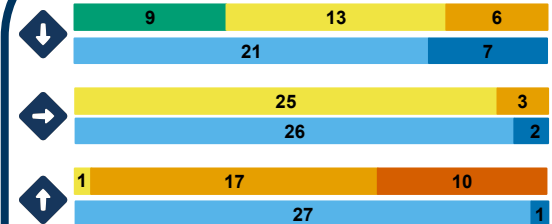
n=28 administrators



19 participants with
>10 years of experience

Findings

Spicing up Defaults



Clarity About the System

“what classifies
‘low’, ‘medium’, and ‘high’”

Understanding of Crucial Terms



Optional MFA



Block