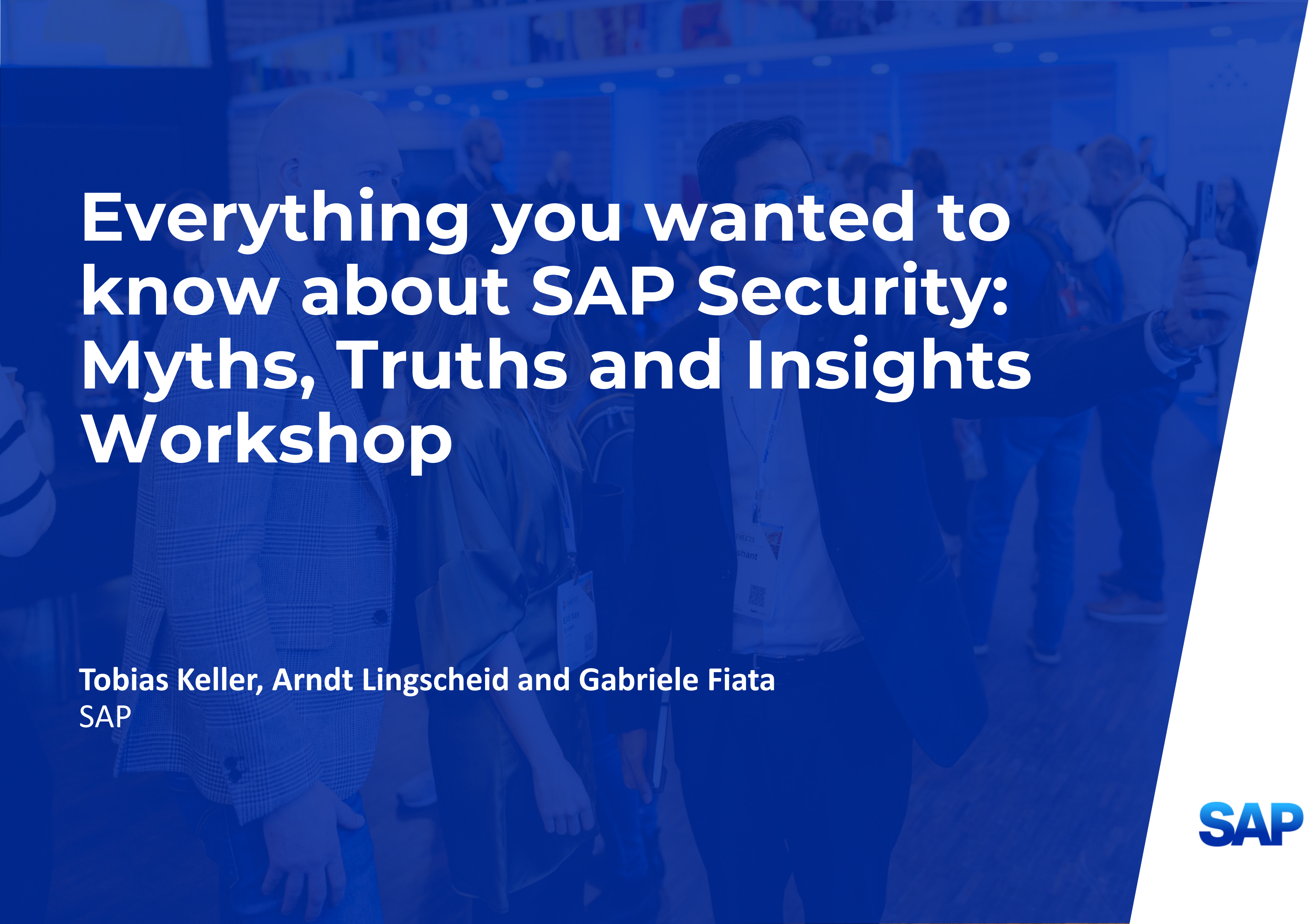


Everything you wanted to know about SAP Security: Myths, Truths and Insights Workshop

Tobias Keller, Arndt Lingscheid and Gabriele Fiata
SAP

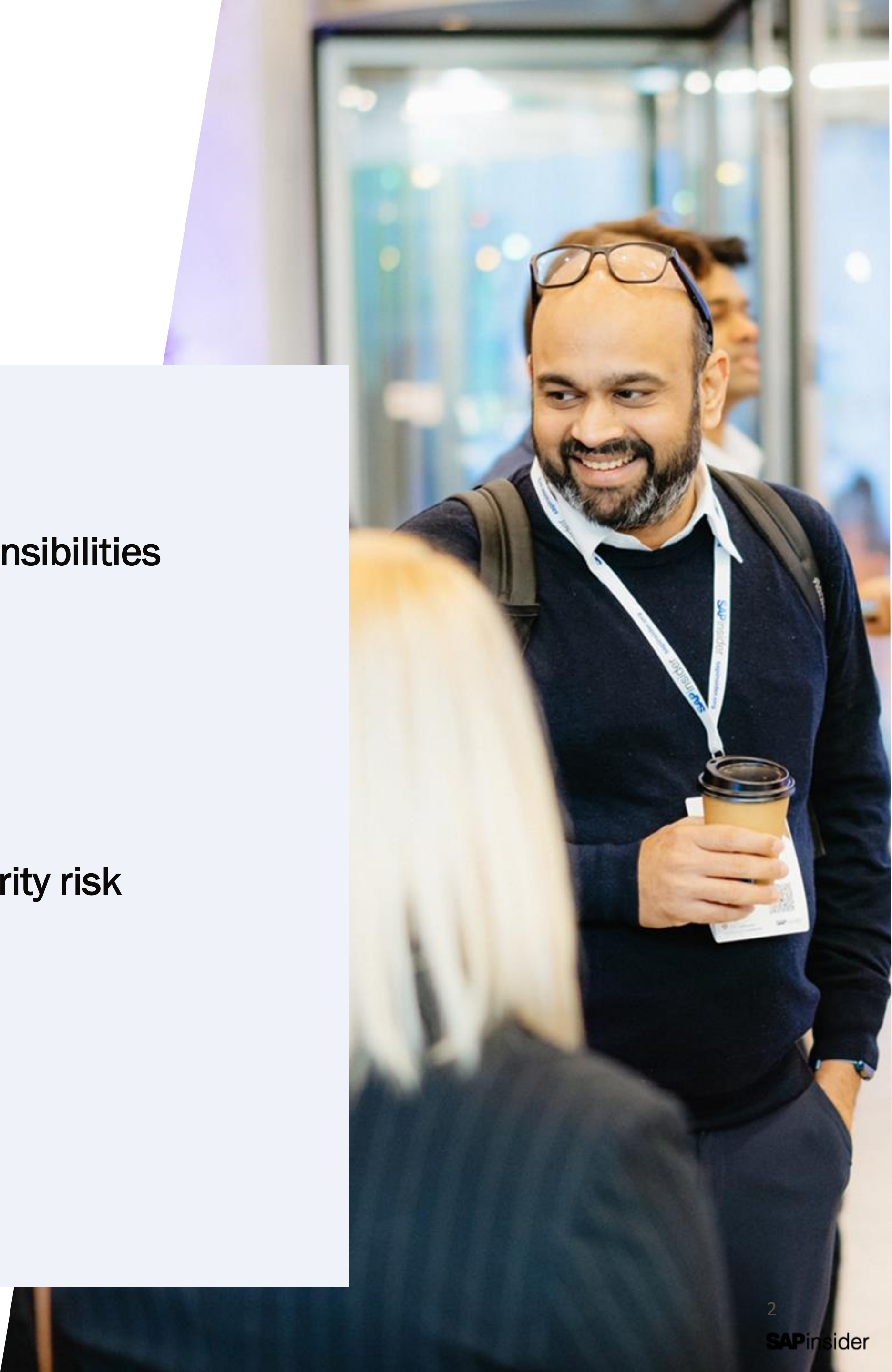
Las Vegas

2024

SAPinsider

What We'll Cover

- Quiz and Intro
- Myth vs Truth - Round 1: Security Focus and Responsibilities
- Coffee and Networking
- Myth vs Truth - Round 2: OnPrem vs Cloud Security
- Myth vs Truth - Round 3: Where is the biggest security risk
- Coffee and Networking
- Wrap-up
- Key points to take home



Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Used by user administrator to maintain User Information.

SU01

(also accepting SU10 as an answer)

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

It defines and manages set of permission for user according to their job responsibilities

PFCG

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Allow users to view detailed information about failed authorization attempts in the SAP GUI

SU53

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Used to display and analyse the security audit log in the SAP system

SM19

(also accepting SM20 as an answer)

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Used for tracing and analysing user activities, RFC calls, HTTP calls and more.

ST01

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Useful for auditing and analysing user authorizations – not dangerous

SUIM

Quiz and Intro – How SAP Security old-school are you?

Guess the tcode:

Useful for auditing and analysing user authorizations – dangerous

SE16

Myth vs Truth - Round 1

Old SAP Security Conversations

Myth vs Truth - Round 1

1. SAP security is mainly the responsibility of the IT department

2. SAP security is mainly about protecting against external threats than internal threats

3. Implementing SAP security measures slows down business performance

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members		
C staff level and business unit managers		
Business Processes		
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	
C staff level and business unit managers		
Business Processes		
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers		
Business Processes		
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	
Business Processes		
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	participate in a risk management committee that meets each month, and information security is always one topic on the agenda.
Business Processes		
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	participate in a risk management committee that meets each month, and information security is always one topic on the agenda.
Business Processes	Business processes are not documented and not analysed for potential risks that can affect operations, productivity, and profitability.	
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	participate in a risk management committee that meets each month, and information security is always one topic on the agenda.
Business Processes	Business processes are not documented and not analysed for potential risks that can affect operations, productivity, and profitability.	Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.
Risk mapping and ownership		

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	participate in a risk management committee that meets each month, and information security is always one topic on the agenda.
Business Processes	Business processes are not documented and not analysed for potential risks that can affect operations, productivity, and profitability.	Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.
Risk mapping and ownership	Risks not assigned to business objectives. Therefore unclear risk ownership.	

SAP security is mainly the responsibility of the IT department

	Company A	Company B
Board Members	do not understand that information security is in their realm of responsibility and focus solely on corporate governance and profits.	understand that information security is critical to the company and demand to be updated regularly on security performance and breaches.
C staff level and business unit managers	think information security is the responsibility of the IT department and the other business units do not get involved.	participate in a risk management committee that meets each month, and information security is always one topic on the agenda.
Business Processes	Business processes are not documented and not analysed for potential risks that can affect operations, productivity, and profitability.	Critical business processes are documented along with the risks that are inherent at the different steps within the business processes.
Risk mapping and ownership	Risks not assigned to business objectives. Therefore unclear risk ownership.	Risks assigned to business objectives. There is clear business risk ownership.

SAP security is mainly about protecting against external threats than internal threats

81% of breaches used lost, stolen or weak passwords.

Three-quarters (75%) of breaches were perpetrated by outsiders, which, of course, means that one-quarter (25%) involved internal actors.

Implementing SAP security measures slows down business performance

“Without brakes we would be driving really, really slowly.”

	Privileged Access Management
Instead of...	Overly complicated workflows to request temporary emergency access
Companies are adopting…	Pre-approved emergency access management with activity logs monitoring and approval.

Implementing SAP security measures slows down business performance

“Without brakes we would be driving really, really slowly.”

	Privileged Access Management	Access Controls
Instead of...	Overly complicated workflows to request temporary emergency access	Removing risky permissions from users to remediate segregation of duties violations.
Companies are adopting...	Pre-approved emergency access management with activity logs monitoring and approval.	- Reveal-on demand with activity logs monitoring - Dinamically Allow/Disallow permissions based on previously performed activities

Implementing SAP security measures slows down business performance

"Without brakes we would be driving really, really slowly."

	Privileged Access Management	Access Controls	Continuous Security Monitoring
Instead of...	Overly complicated workflows to request temporary emergency access	Removing risky permissions from users to remediate segregation of duties violations.	Over restricting sensitive access from users to avoid critical incidents.
Companies are adopting...	Pre-approved emergency access management with activity logs monitoring and approval.	- Reveal-on demand with activity logs monitoring - Dinamically Allow/Disallow permissions based on previously performed activities	Monitor suspicious activities and implement system auto-reactions to block users when surpassing certain risk thresholds

Coffee and Networking

…or personal time…

Myth vs Truth - Round 2

OnPrem vs Cloud Security

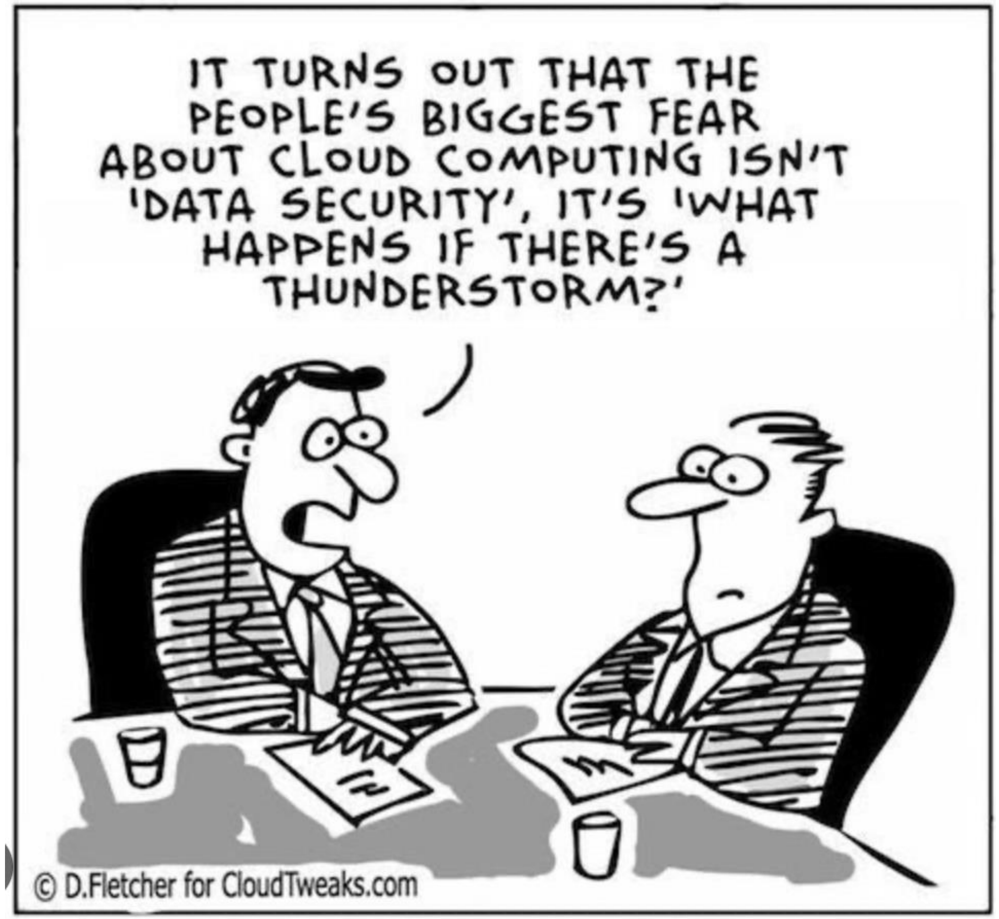
Myth vs Truth - Round 2

1. SAP systems, on-premises, are inherently more secure than their cloud counterparts

2. Securing data in SAP cloud systems presents greater challenges compared to on-premise solutions.

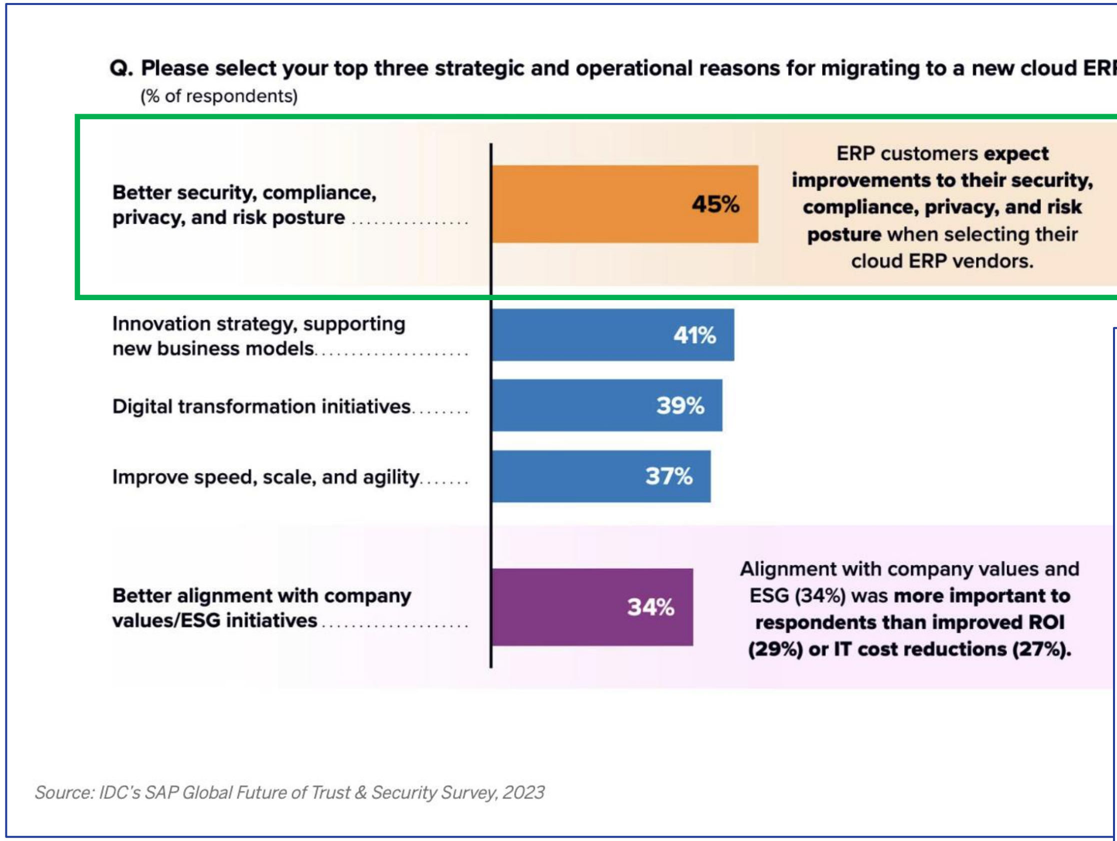
3. The security advantages of SAP Cloud solutions are undeniably clear.

SAP systems, on-premises, are inherently more secure than their cloud counterparts


IT TURNS OUT THAT THE PEOPLE'S BIGGEST FEAR ABOUT CLOUD COMPUTING ISN'T 'DATA SECURITY', IT'S 'WHAT HAPPENS IF THERE'S A THUNDERSTORM?'
© D.Fletcher for CloudTweaks.com

Parameters	Cloud Security	On-premise Security
Cost	Eliminates the necessity for businesses to make costly investments in hardware, software, and IT personnel	Responsible for the expenses associated with the installation, maintenance, and upgrades of hardware and software
Scalability	Can easily scale up or down their security requirements according to their changing needs	Cannot easily adjust their security needs according to their evolving requirements
Reliability	Invest heavily in robust security infrastructure and backup systems	Susceptible to hardware failures, power outages, and other system failures
Control	Limits control over their security infrastructure	Complete control over their hardware and software
Deployment Time	With the advantage of pre-configured security settings, deployment can be achieved much more quickly	Involves the installation and configuration of security infrastructure, which can be a time-consuming process

Securing data in SAP cloud systems presents greater challenges compared to on-premise solutions.

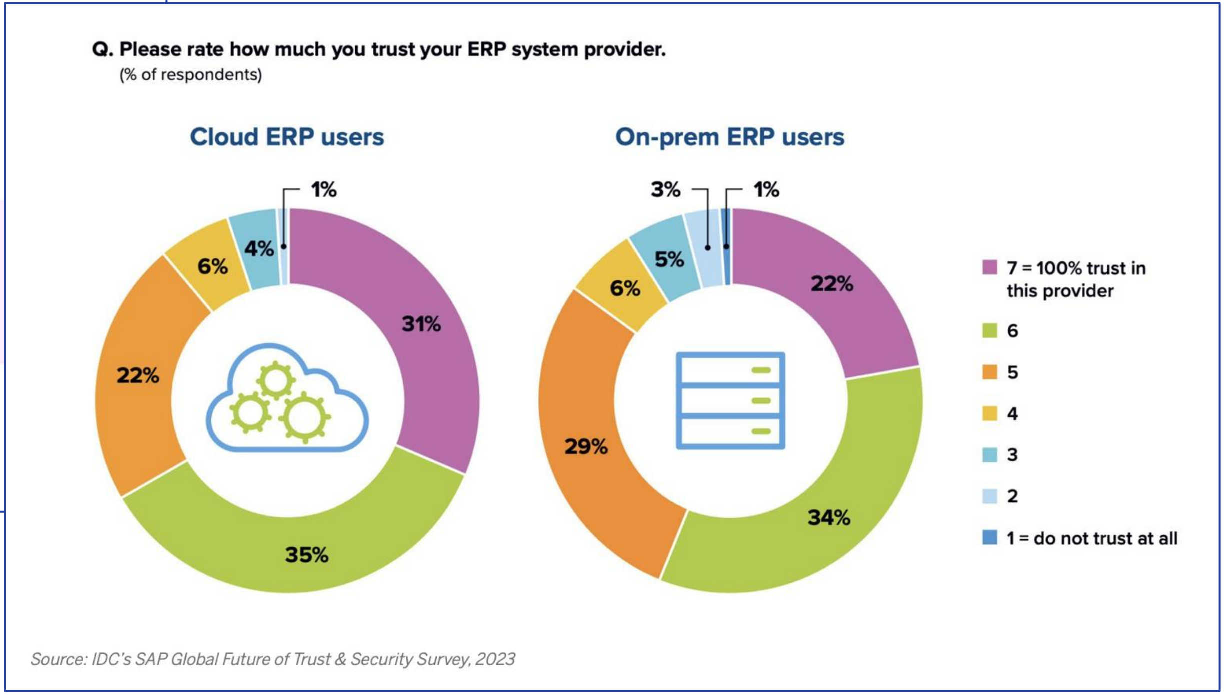


Q. Please select your top three strategic and operational reasons for migrating to a new cloud ERP system.
(% of respondents)

ERP customers **expect improvements to their security, compliance, privacy, and risk posture** when selecting their cloud ERP vendors.

Alignment with company values and ESG (34%) was **more important to respondents than improved ROI (29%) or IT cost reductions (27%).**

Source: IDC's SAP Global Future of Trust & Security Survey, 2023



Q. Please rate how much you trust your ERP system provider.
(% of respondents)

Source: IDC's SAP Global Future of Trust & Security Survey, 2023

The security advantages of SAP Cloud solutions are undeniably clear.

I HAVE A PARTICULAR SET OF SKILLS...
NETWORK SECURITY, CLOUD SOLUTIONS, DATA RECOVERY, AND 24/7 MANAGED SERVICES
imgflip.com

Cost of global cybercrime by 2025?

cyber and data security risks
and threats are skyrocketing.

Myth vs Truth - Round 3

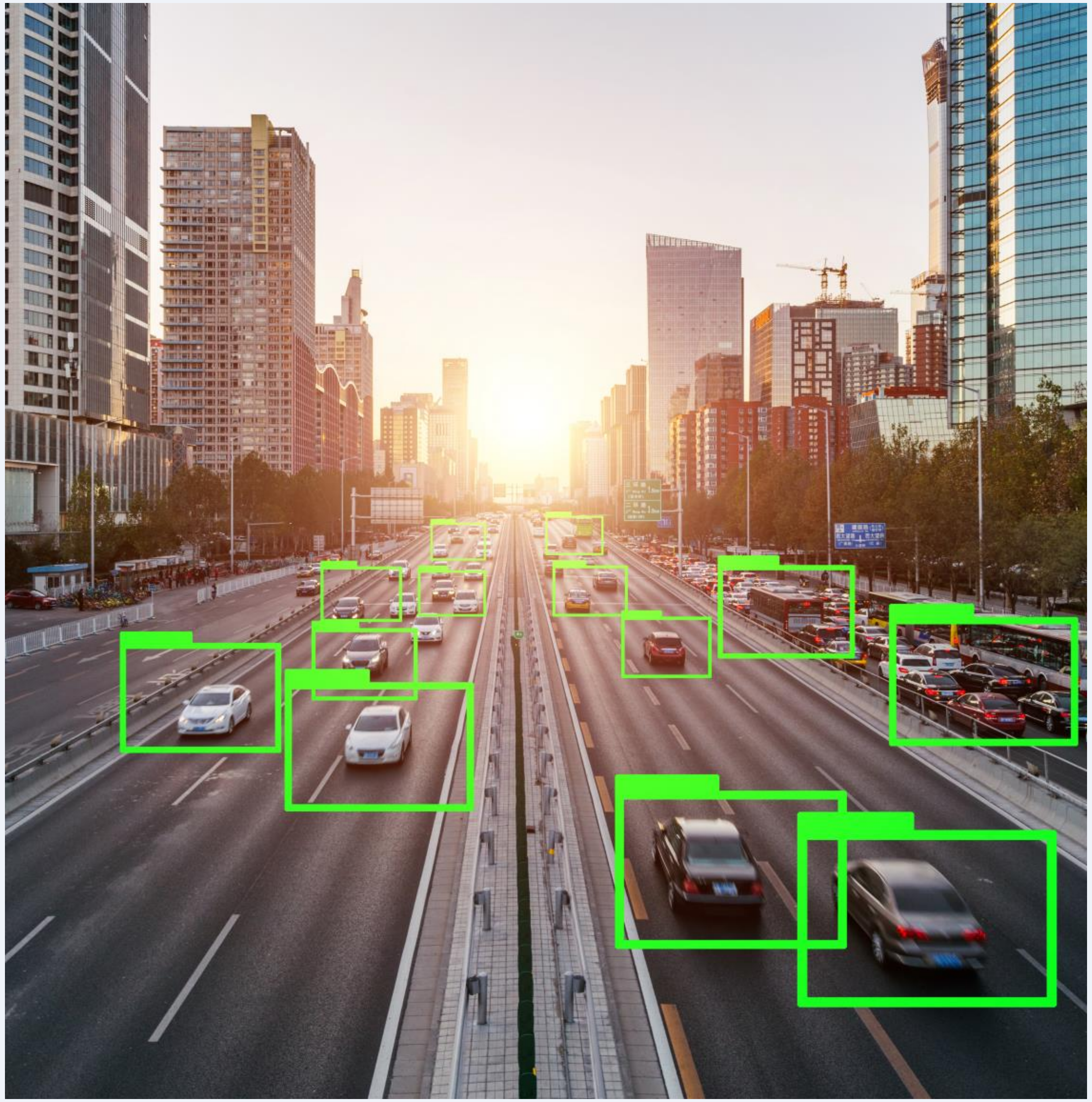
New SAP Security Conversations

Myth vs Truth - Round 3

1. Security audits are necessary for compliance; they don't significantly improve overall SAP security.

2. Every cyber threat facing the company must be effectively mitigated through the implementation of robust controls.

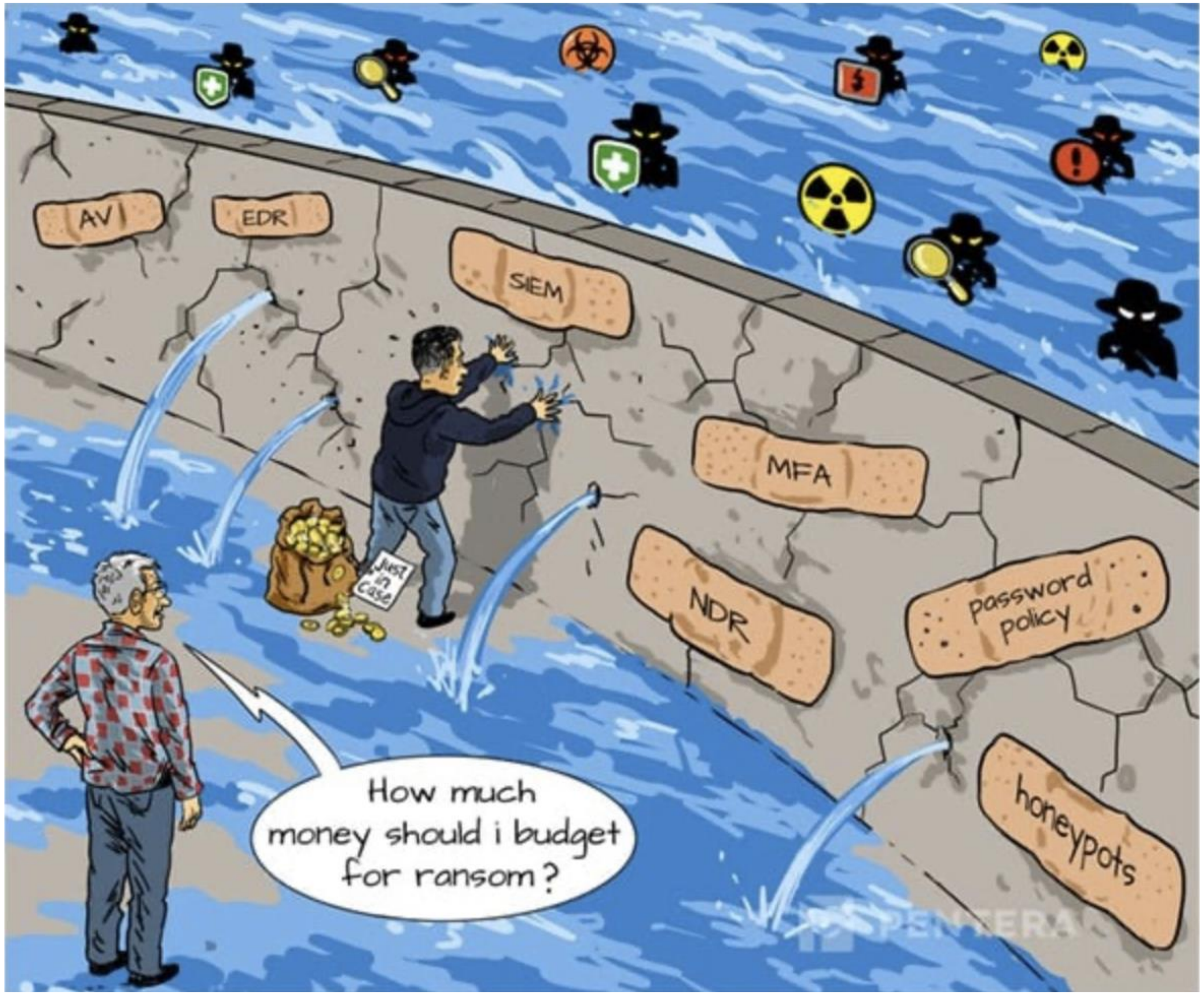
3. AI and LLMs provide attackers with powered offensive capabilities, significantly surpassing traditional hacking methods



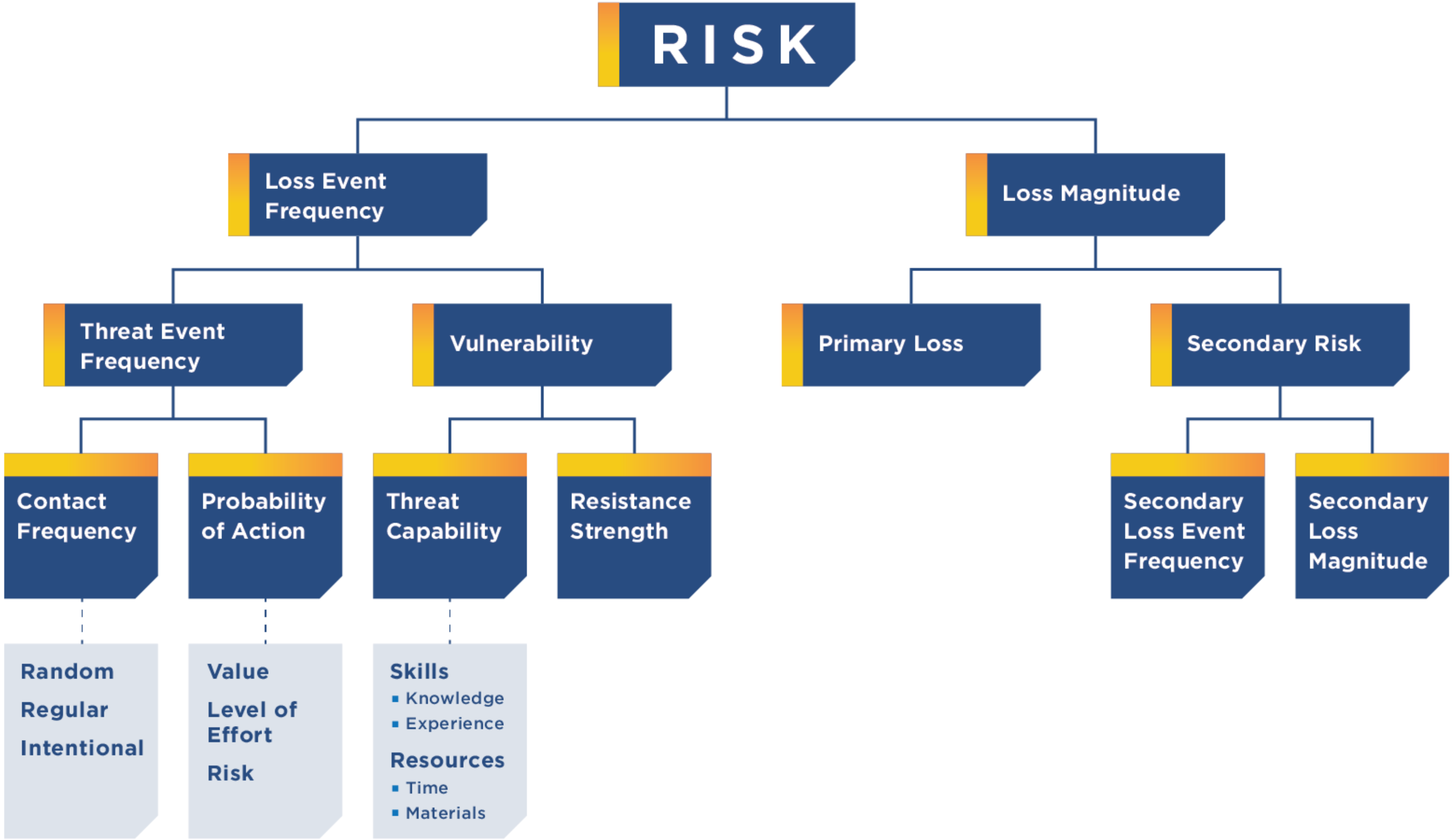
Security audits are necessary for compliance; they don't significantly improve overall security

Usually checked by Audit	Usually Not Checked by Audit
Switch on the SAP Security Audit Log	Monitoring the SAP Security Audit Log with a formal process
SAP systems are set to not-modifiable	Modifying ABAP code directly in PRD (system does not need to be open to do it)
No users with SAP_ALL	Checking reports and functions with no authorization checks

Every cyber threat facing the company must be effectively mitigated through the implementation of robust controls.



Every cyber threat facing the company must be effectively mitigated through the implementation of robust controls.



AI and LLMs provide attackers with powered offensive capabilities, significantly surpassing traditional hacking methods.

USING LLMs TO DEVELOP MALWARE

- Uncertain if LLM-based tools offer advantages over traditional hacking resources
- Potential risk: increase in attackers, decrease in effort needed to develop malicious tools
- Most LLMs trained on easily accessible public resources
- LLMs' generalization may not significantly enhance offensive capabilities

LLMs FOR SOCIAL ENGINEERING

- Scammers can enhance grammar, prose, and content randomization in phishing emails.
- LLMs streamlines spear phishing attacks, increasing their quantity, if not quality.
- With technologies like voice synthesis and text/image generators, LLMs can impersonate specific speech styles and voices, facilitating social engineering, vishing attacks and manipulation of targets.

Coffee and Networking

…or personal time…

We start again in 15 minutes.

Wrap-up

Parked questions

Key Points to Take Home

To be done together as part of the workshop

Where to Find more Information

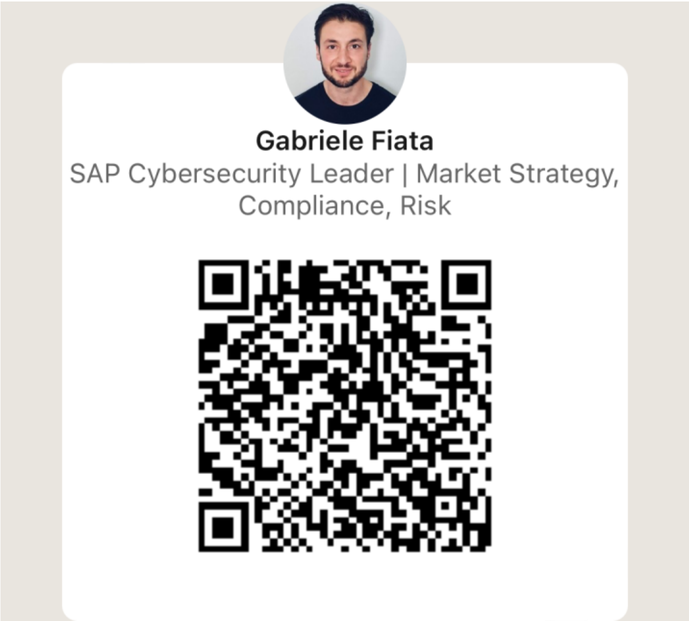
- ERP Today Article: From NO to YES, but securely
- SAP Insights Article on IDC Research: Building Better Trust in Business with Cloud ERP Investments
- SAP Cloud ERP Security Video
- RISE with SAP Security Brief
- GROW with SAP Security Brief
- Demystifying Cyber Risk: Empowering SAP Organizations to Measure and Integrate Cyber Risks into Business Decisions

Thank you! Any Questions?

Please remember to complete your session evaluation.

Arndt Lingscheid
Global Solution Owner Cybersecurity and Dataprotection, Product Management at SA...

Tobias Keller (莊德凱)
Product Manager | Transforming customer orientation into product innovation and gro...



Gabriele Fiata
SAP Cybersecurity Leader | Market Strategy, Compliance, Risk

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.