Tips to Implement MFA for Your SAP Applications

John Mortimer, Consultant, CyberSafe

SAPinsider
Las Vegas

2023

CyberSafe

In This Session

Why we need MFA

Where you need to use it

How to implement it in an SAP landscape

Speaker

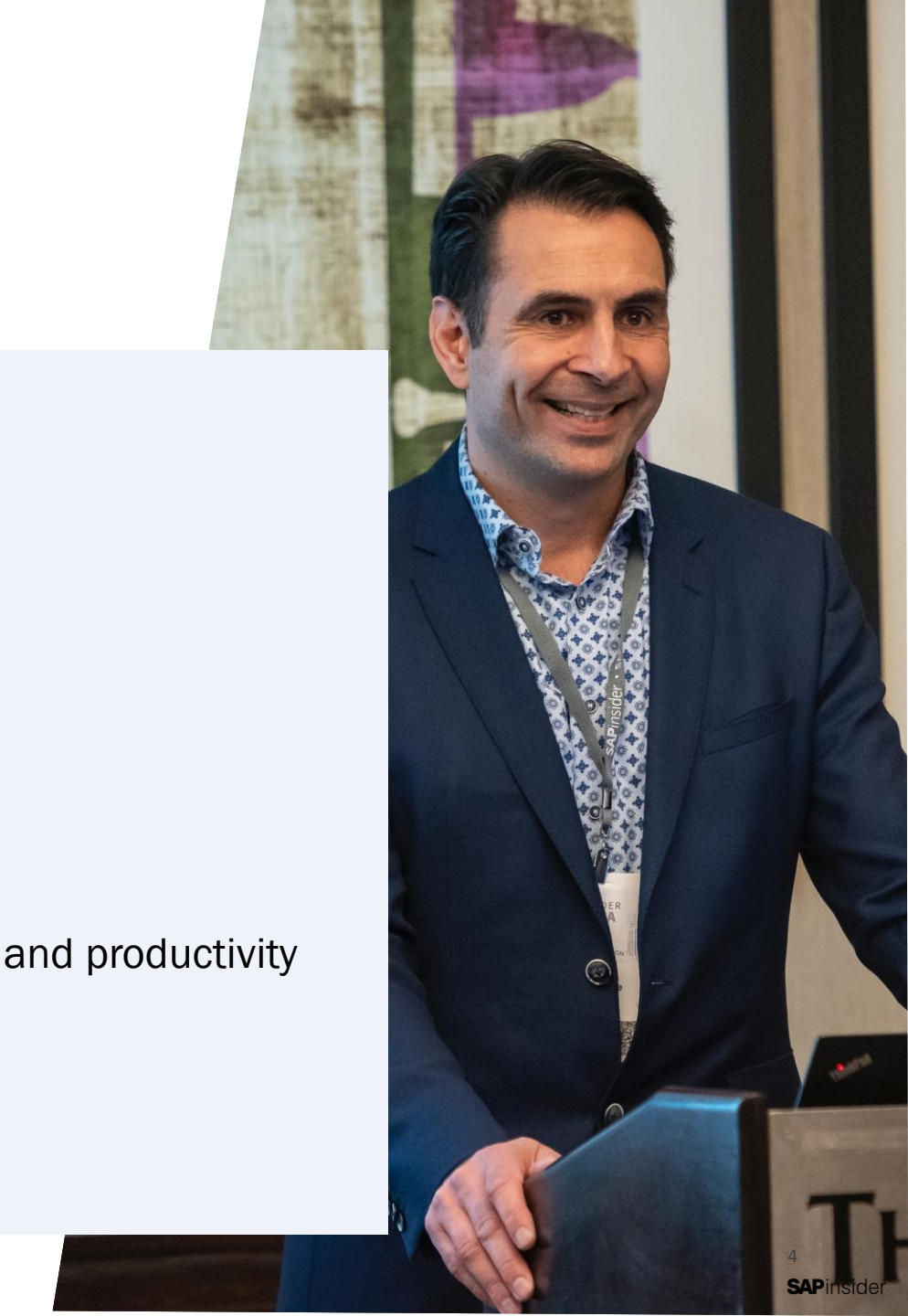
John Mortimer
Security Consultant

Tel: +44 7766770261
Email: John.Mortimer@CyberSafe.com

CyberSafe

What We'll Cover

- About CyberSafe
- The SAP Security Challenge
- Top Security Mistakes in SAP environments
  - Password Issues
  - Weak user access controls
- Zero Trust
- MFA - The pros and cons
- How to use SSO with MFA to maximize security and productivity
- Wrap up

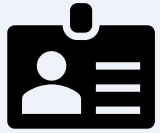


About CyberSafe

SAP® PartnerEdge Partner

SAP Certified products

29+ years experience



TrustBroker® products used for flexible SAP user authentication (SSO and MFA)

Enterprise customers worldwide

from 5-100,000 users

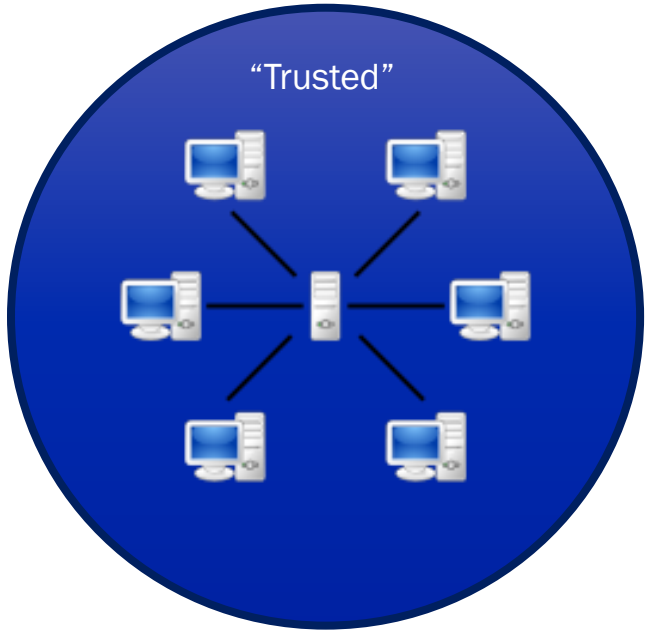
The SAP Security Challenge

CyberSafe

The SAP Security Challenge

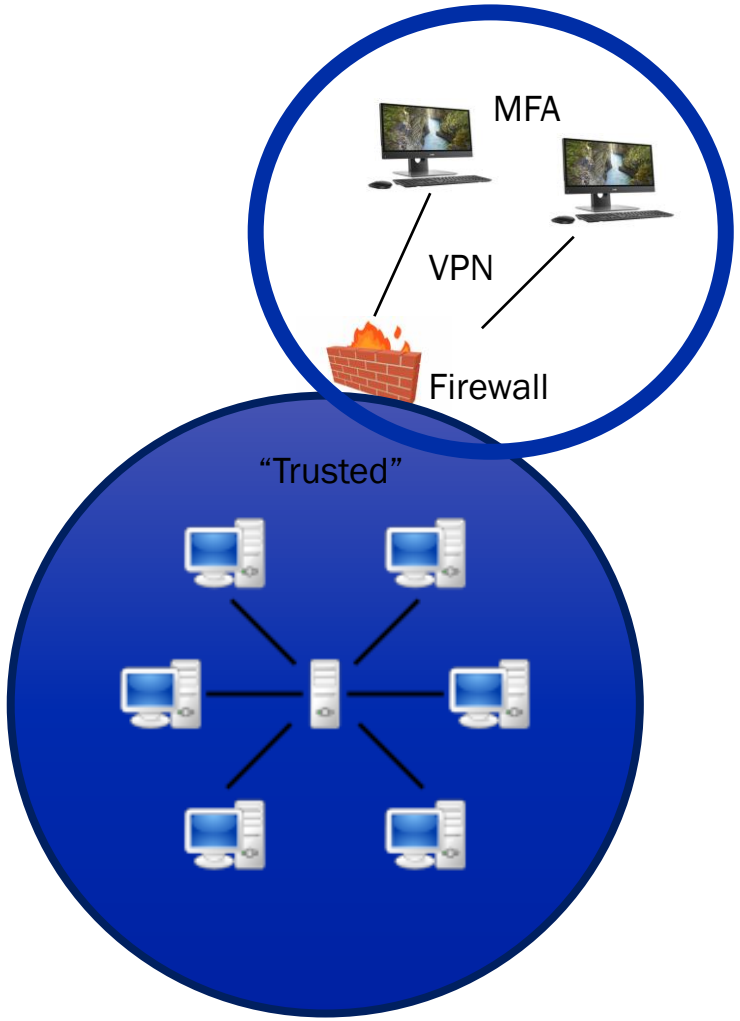
- SAP systems often hold the company's most valuable data
- Traditionally, SAP products were not fully integrated with enterprise security
- SAP systems are now fully connected to the Internet and vulnerable to outside attacks.

Traditional Network Security



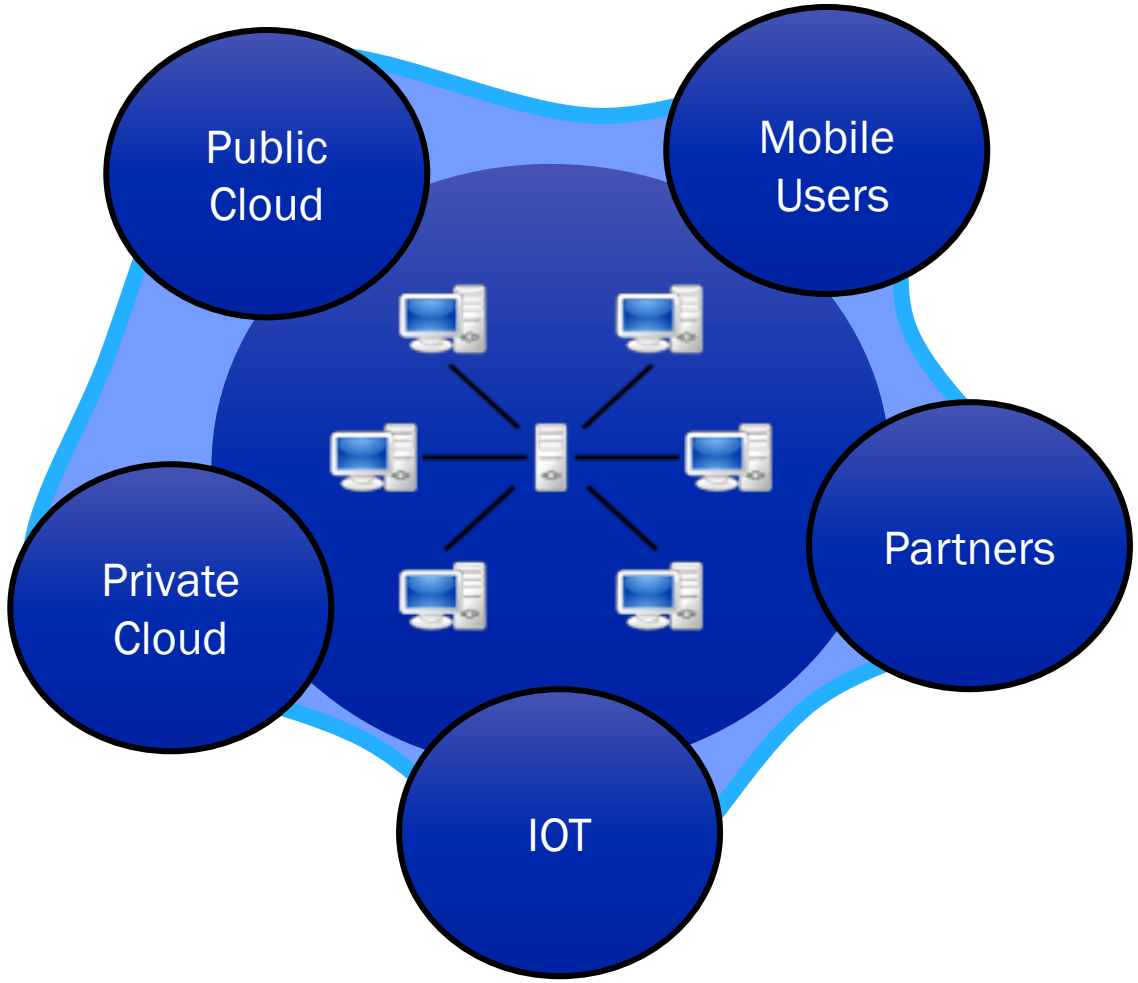
CyberSafe

Perimeter Based Security



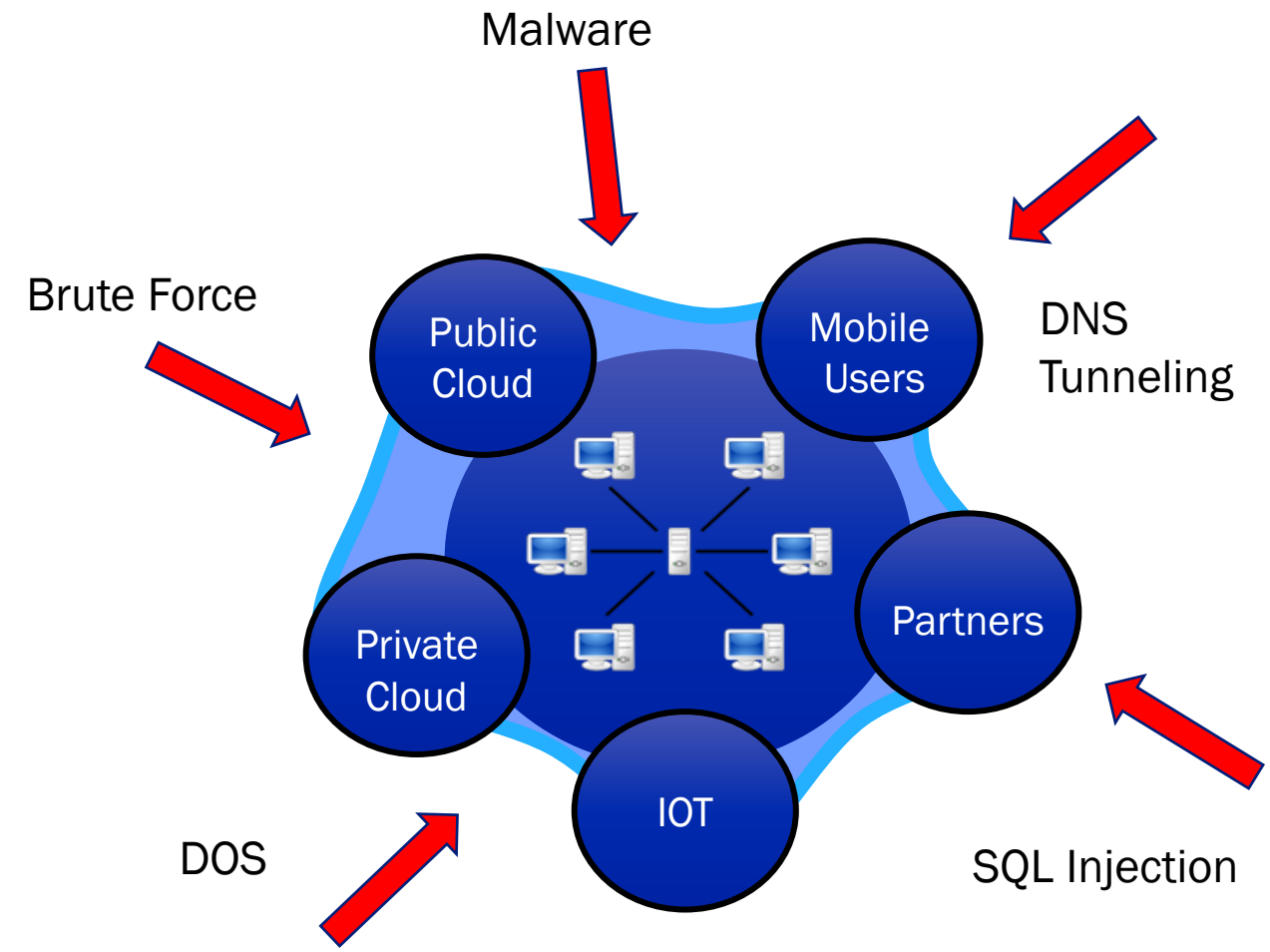
CyberSafe

Where is the new perimeter?

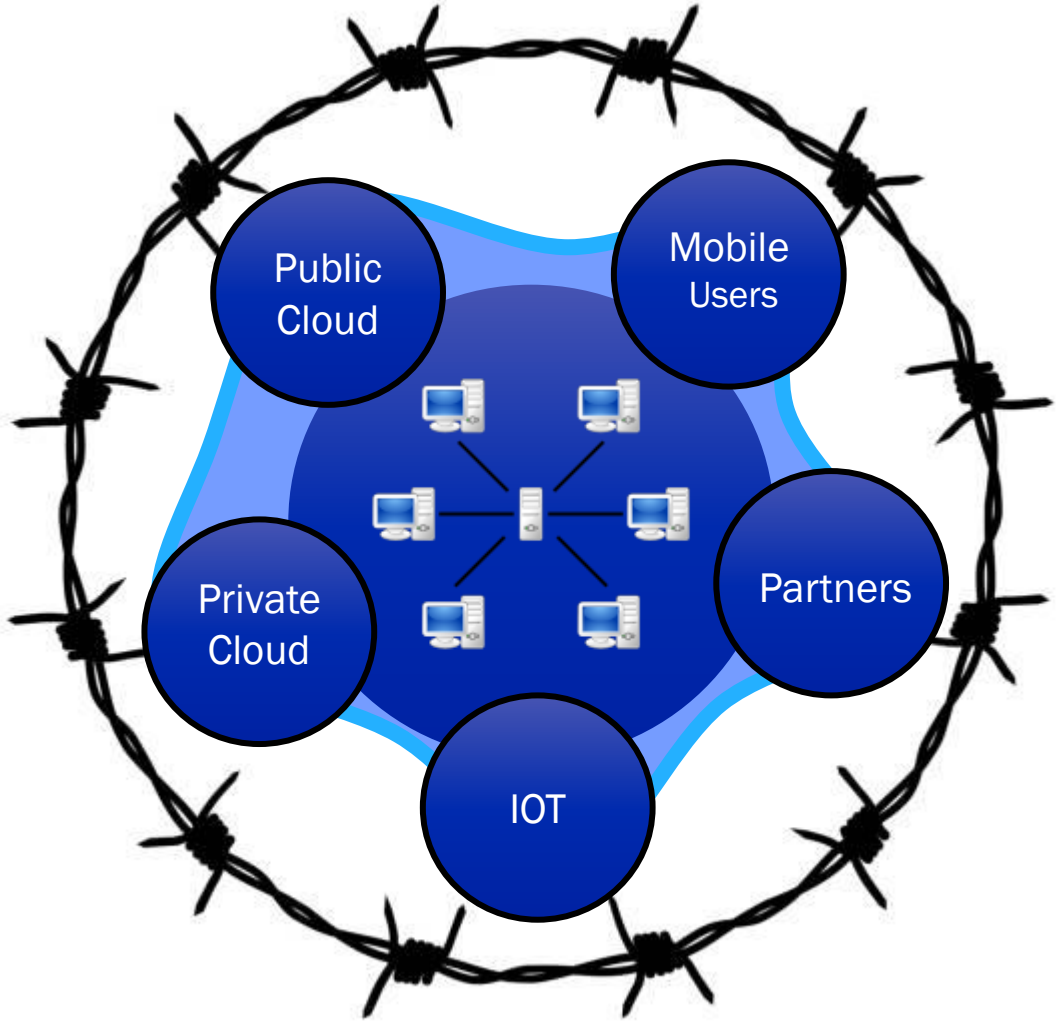


Source: https://onapsis.com/press-releases/independent-market-survey-reveals-64-erp-deployments-have-been-breached-last-24

What is an Outsider Attack?



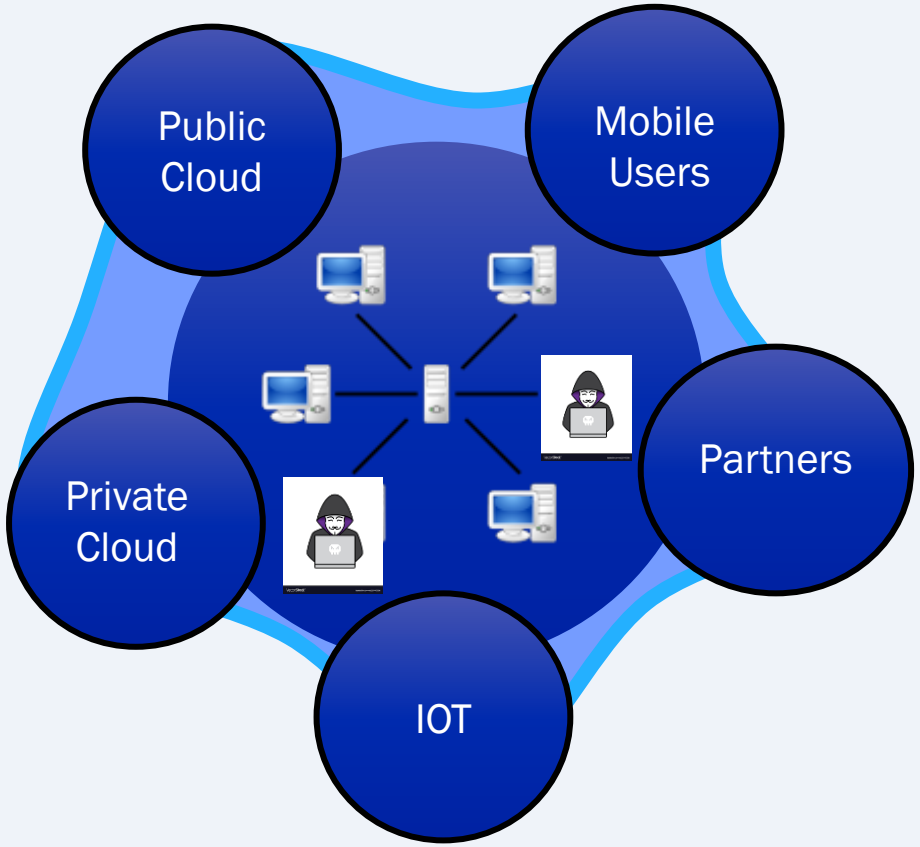
Outsider attack prevention



CyberSafe

Insider Attacks

A malicious attack on an organization comes from people within the organization (such as employees, former employees, contractors or business associates) who have inside information concerning the organization's security practices, data and computer systems.



Source: https://en.wikipedia.org/wiki/Insider_threat

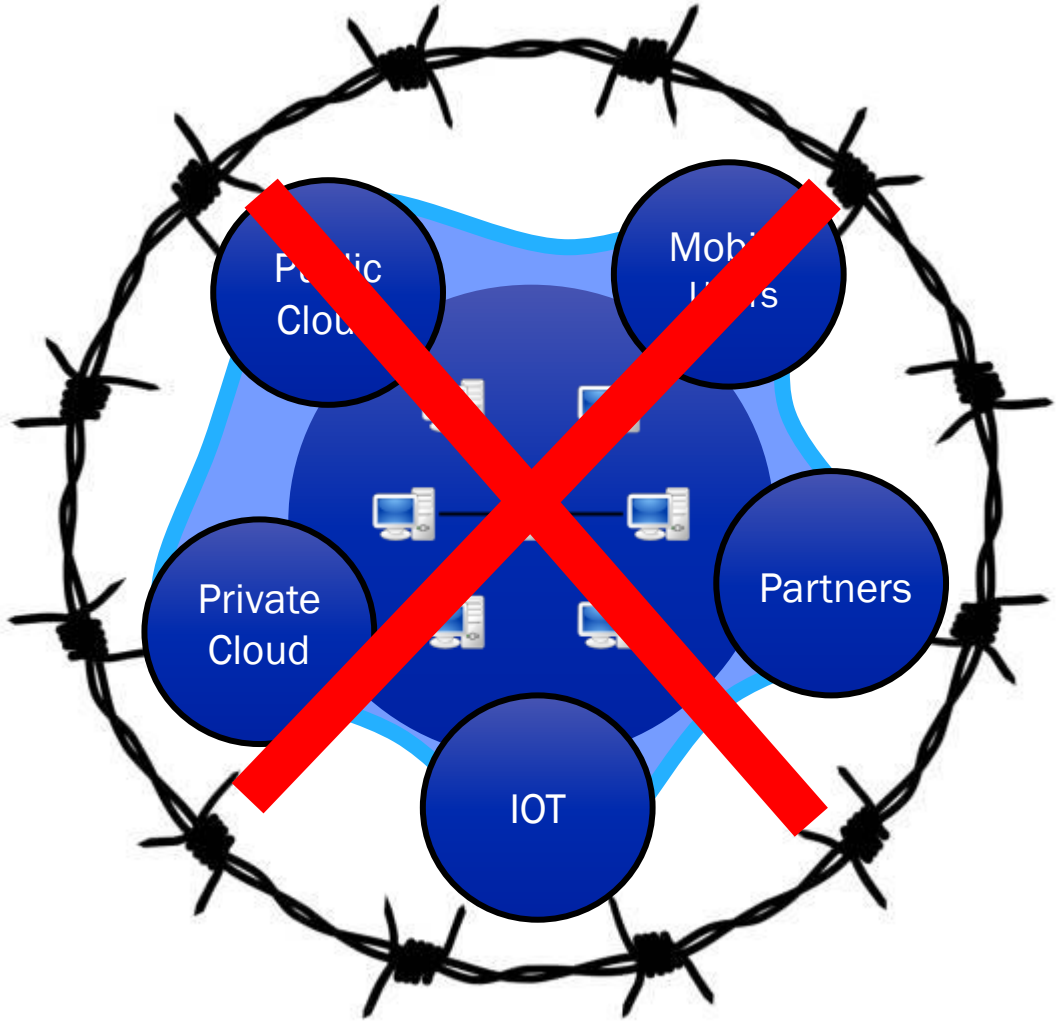
33% of all data breaches are Insider Attacks

- **Negligent insiders,** or employees or contractors who make mistakes that unintentionally cause incidents.
- **Criminal and malicious insiders**, or those who intentionally cause damage to an organization from the inside.
- **Infiltrators/Credential thieves,** or those who target insiders' login information to gain unauthorized access to applications and systems.

  Infiltrators/credential thieves cause the most damage, costing organizations an average of nearly $3 million per year.

Source: https://go.forrester.com/predictions/

Trusted Zone Security is no longer valid



CyberSafe

Cyber Crime Continues to grow

In the last 5 years:

Cybercrime has increased by 67%
Cost of each cyber breach increased 72% to $13.3m

Source: 9th Annual Cost of Cybercrime Study, conducted by Accenture Security and the Ponemon Institute
https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Top Security Mistakes

CyberSafe

Security Mistakes in SAP environments

- Poor password management
- Weak user access controls
- Sloppy patch management…
- Misconfigured ACLs…
- Insecure custom code…
- Unprotected data…
- Inadequate logging and auditing…
- Failure to have an emergency response plan…

Source: https://www.csoonline.com/article/3404470/top-8-security-mistakes-in-sap-environments.html

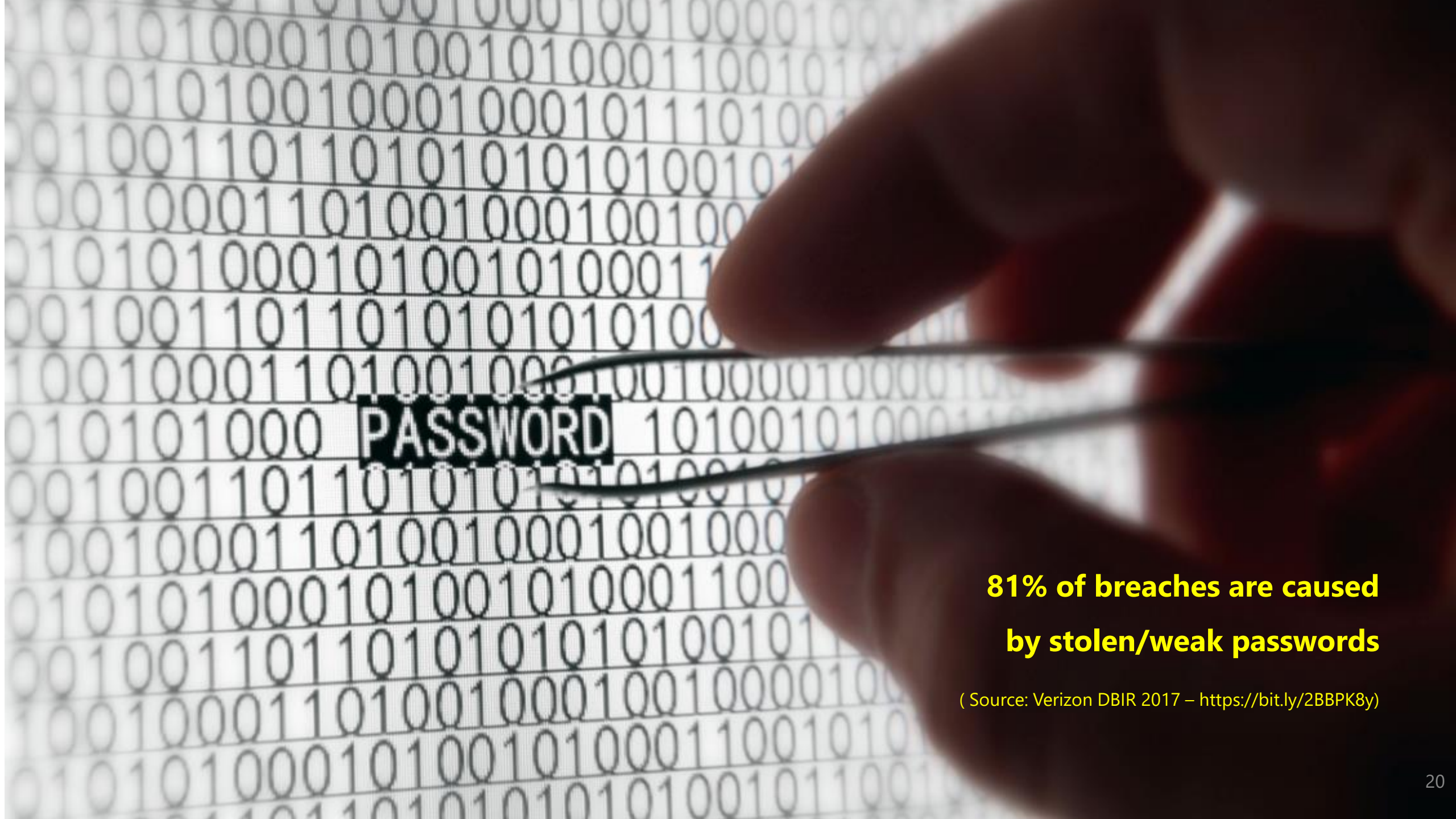
CyberSafe

Security Mistakes in SAP environments

- Poor password management
- Weak user access controls
- Sloppy patch management…
- Misconfigured ACLs…
- Insecure custom code…
- Unprotected data…
- Inadequate logging and auditing…
- Failure to have an emergency response plan…

Source: https://www.csoonline.com/article/3404470/top-8-security-mistakes-in-sap-environments.html

CyberSafe



81% of breaches are caused by stolen/weak passwords

(Source: Verizon DBIR 2017 – https://bit.ly/2BBPK8y)

The Solution – Strong Passwords?

6Qf8Ue%f5&R!z`

Users like memorable passwords

2007

1. password
2. 123456
3. qwerty
4. abc123
5. letmein

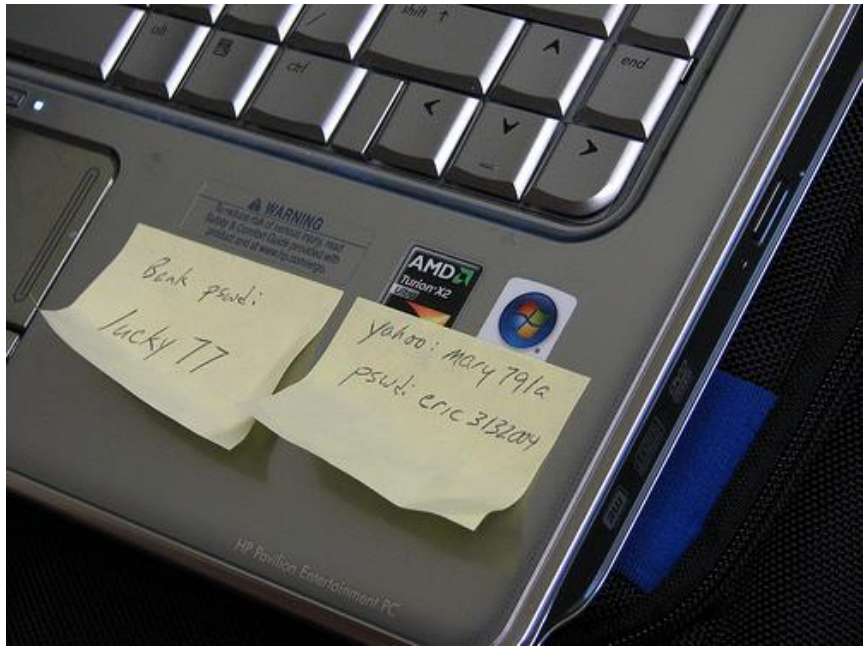
2020

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345

Source: https://cybernews.com/best-password-managers/most-common-passwords/

Methods of credentials exploitation

- Negligence and poor practices



Source: https://nordpass.com/most-common-passwords-list/

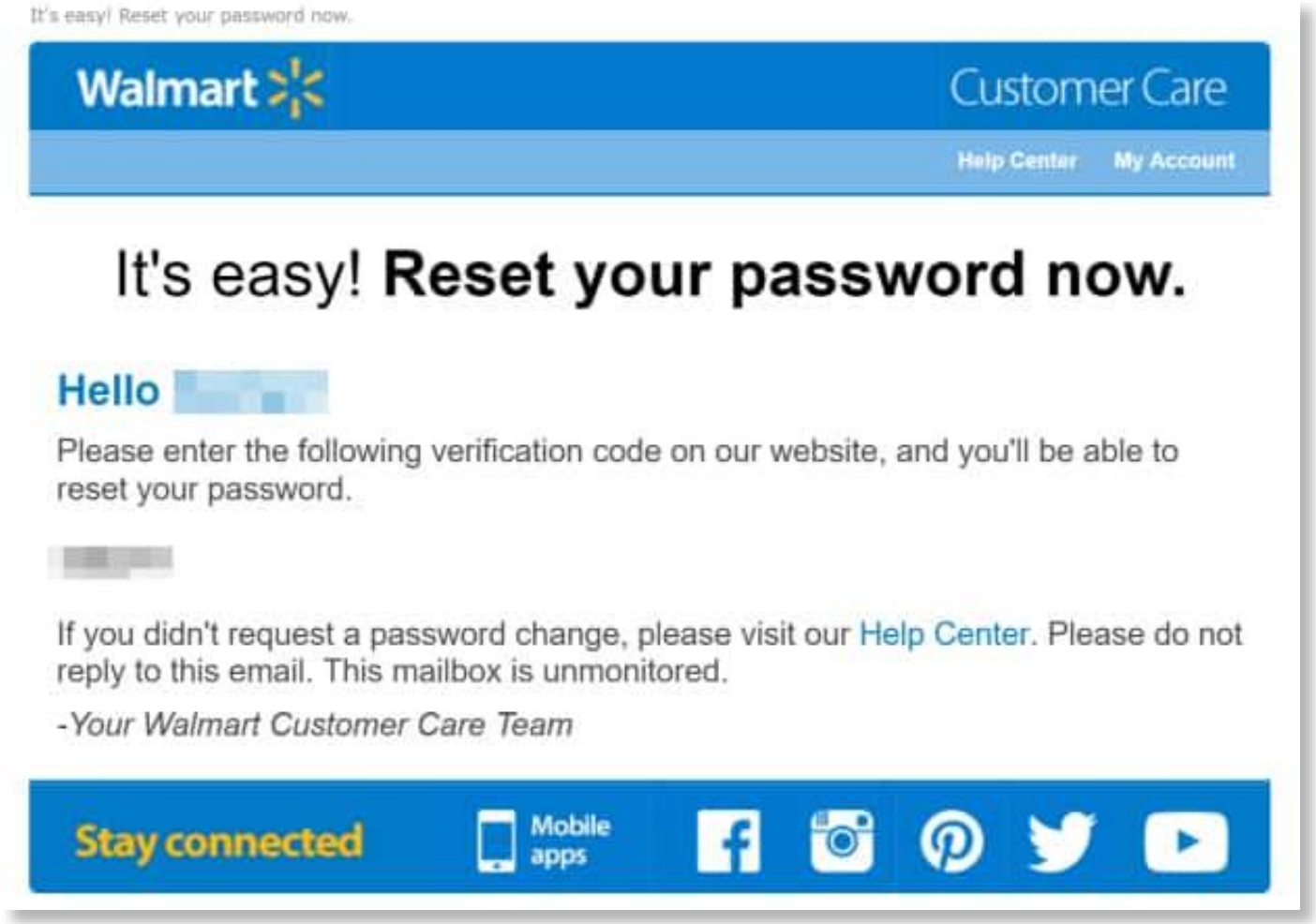
Social Engineering

Methods of credential exploitation

- Credential thieves
- Phishing
- Spear Phishing
- Vishing

CyberSafe

Social Engineering - Phishing example



Weak User Access Controls

- Privileged Users
  - Targeted by hackers

- Joiners, Movers and Leavers (JML)
  - Permission Creep
  - Developers/Contractors
  - Leavers
    - Dismissed employee
    - Notice period

SAP Data Breach Example

CyberSafe

SAP Data Breach - Example

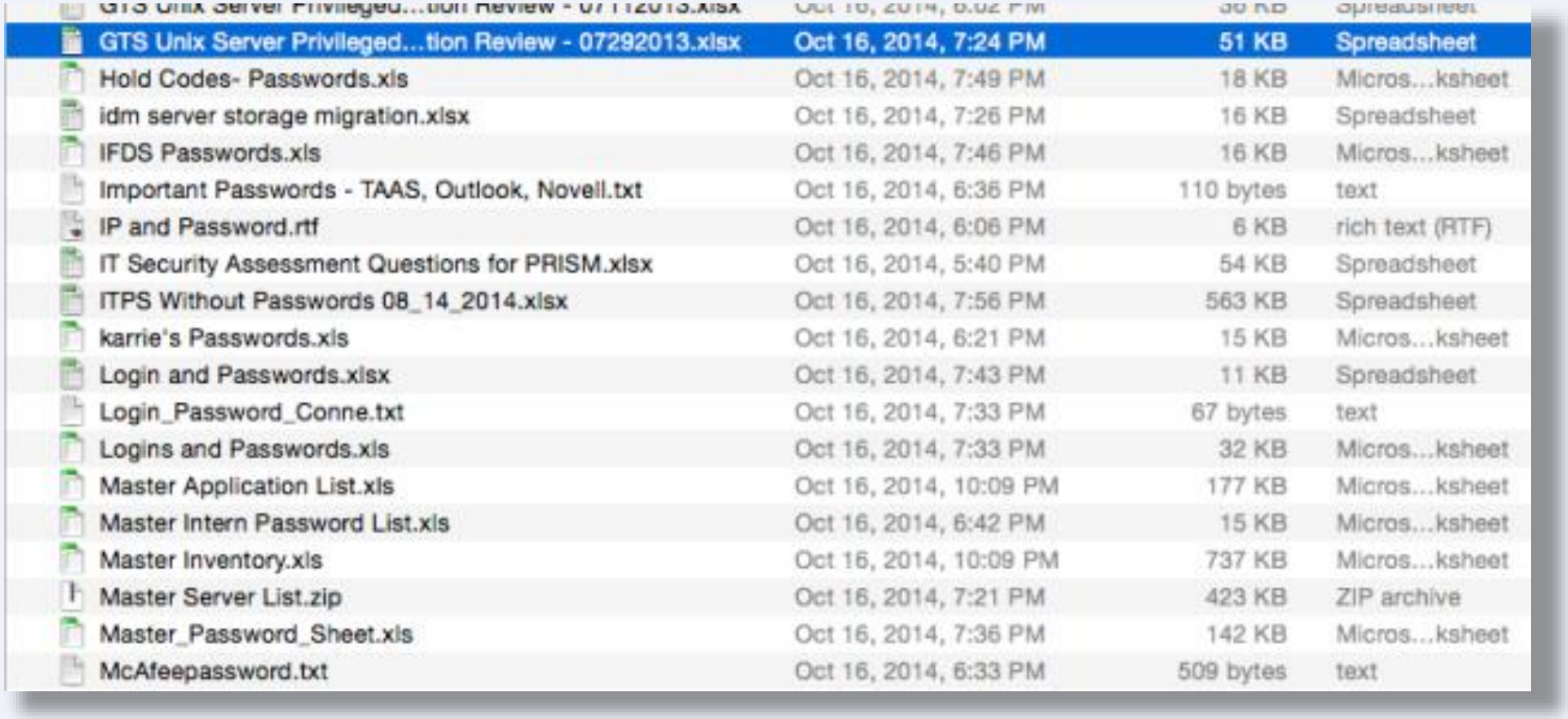
Sony Pictures Entertainment

- Hacked by North Korea in 2014, initially by Malware
- Username and password combinations stored in cleartext

Source: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

SAP Data Breach - Example

Sony Pictures Entertainment

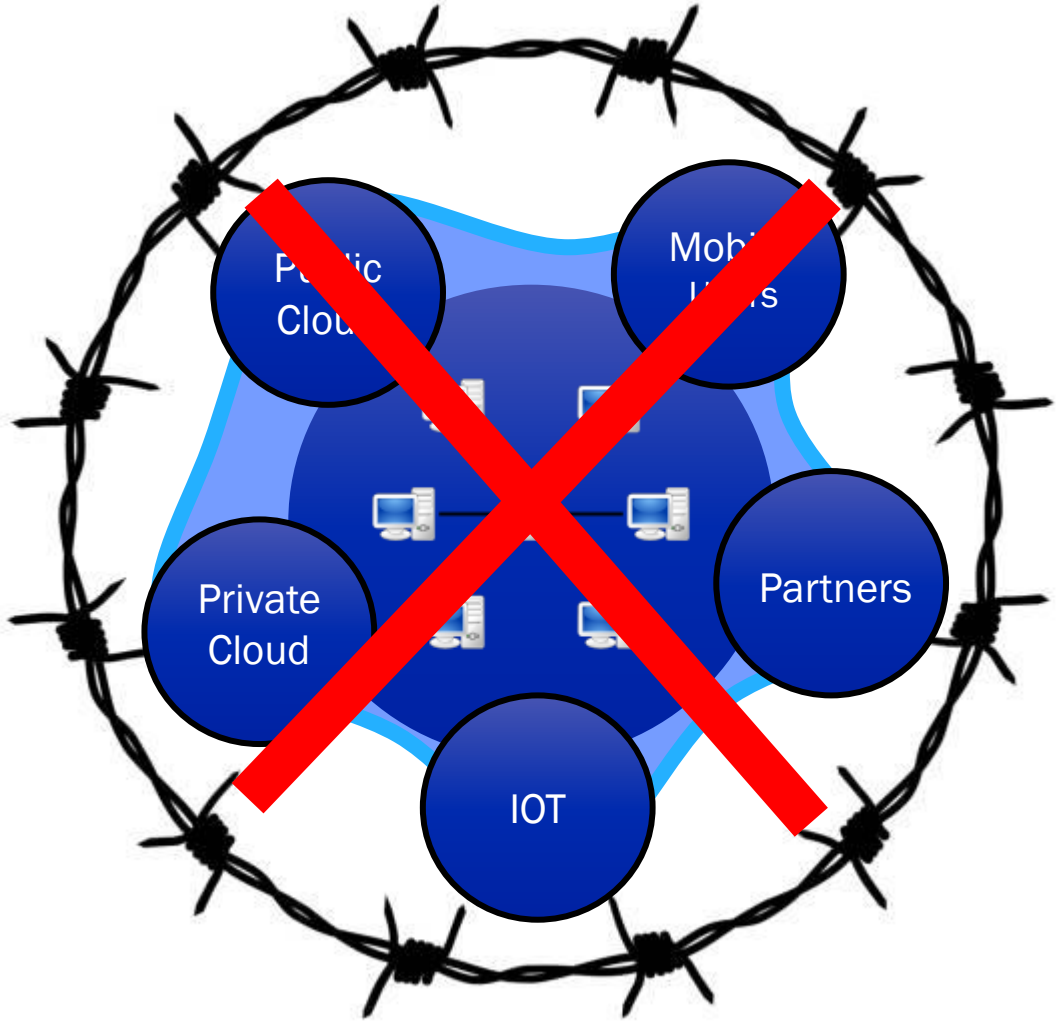


GTS Unix Server Privileged...tion Review - 07292013.xlsx	Oct 16, 2014, 7:24 PM	51 KB	Spreadsheet
Hold Codes- Passwords.xls	Oct 16, 2014, 7:49 PM	18 KB	Micros...ksheet
idm server storage migration.xlsx	Oct 16, 2014, 7:26 PM	16 KB	Spreadsheet
IFDS Passwords.xls	Oct 16, 2014, 7:46 PM	16 KB	Micros...ksheet
Important Passwords - TAAS, Outlook, Novell.txt	Oct 16, 2014, 6:36 PM	110 bytes	text
IP and Password.rtf	Oct 16, 2014, 6:06 PM	6 KB	rich text (RTF)
IT Security Assessment Questions for PRISM.xlsx	Oct 16, 2014, 5:40 PM	54 KB	Spreadsheet
ITPS Without Passwords 08_14_2014.xlsx	Oct 16, 2014, 7:56 PM	563 KB	Spreadsheet
karrie's Passwords.xls	Oct 16, 2014, 6:21 PM	15 KB	Micros...ksheet
Login and Passwords.xlsx	Oct 16, 2014, 7:43 PM	11 KB	Spreadsheet
Login_Password_Conne.txt	Oct 16, 2014, 7:33 PM	67 bytes	text
Logins and Passwords.xls	Oct 16, 2014, 7:33 PM	32 KB	Micros...ksheet
Master Application List.xls	Oct 16, 2014, 10:09 PM	177 KB	Micros...ksheet
Master Intern Password List.xls	Oct 16, 2014, 6:42 PM	15 KB	Micros...ksheet
Master Inventory.xls	Oct 16, 2014, 10:09 PM	737 KB	Micros...ksheet
Master Server List.zip	Oct 16, 2014, 7:21 PM	423 KB	ZIP archive
Master_Password_Sheet.xls	Oct 16, 2014, 7:36 PM	142 KB	Micros...ksheet
McAfeepassword.txt	Oct 16, 2014, 6:33 PM	509 bytes	text


"Hackers don't break in,
they log in."
Bret Arsenault
Chief Information Security Officer (CISO)
Microsoft

Zero Trust

Trusted Zone Security is no longer valid



CyberSafe

The future – Zero Trust

White House instructs all agencies to adopt a zero trust approach to cybersecurity

While the concept behind zero trust is not new, the implications of shifting away from "trusted networks" are new to most enterprises …

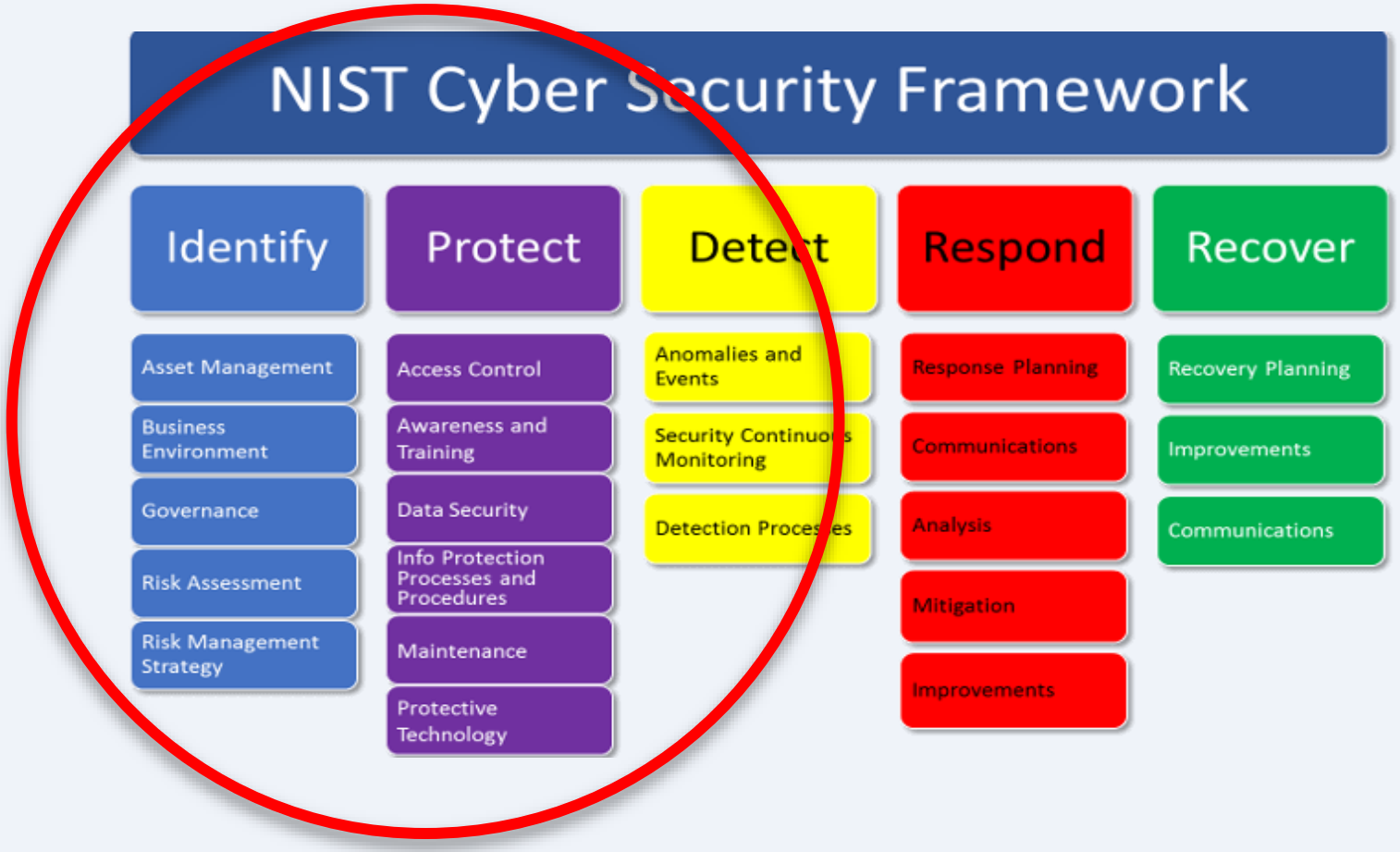
The strategy requires agencies to meet objectives by the end of 2024. In addition, the strategy places a significant emphasis on stronger enterprise identity and access controls, **including multi-factor authentication (MFA) …**

Source: https://www.securitymagazine.com/articles/96987-white-house-instructs-agencies-to-adopt-zero-trust-approach-to-cybersecurity

There is no Trusted Zone – so assume Zero Trust

1. Focus on Critical Data
2. Limit who has access
3. Stop relying on passwords
4. Use MFA to authenticate users

Prevention is better than the cure



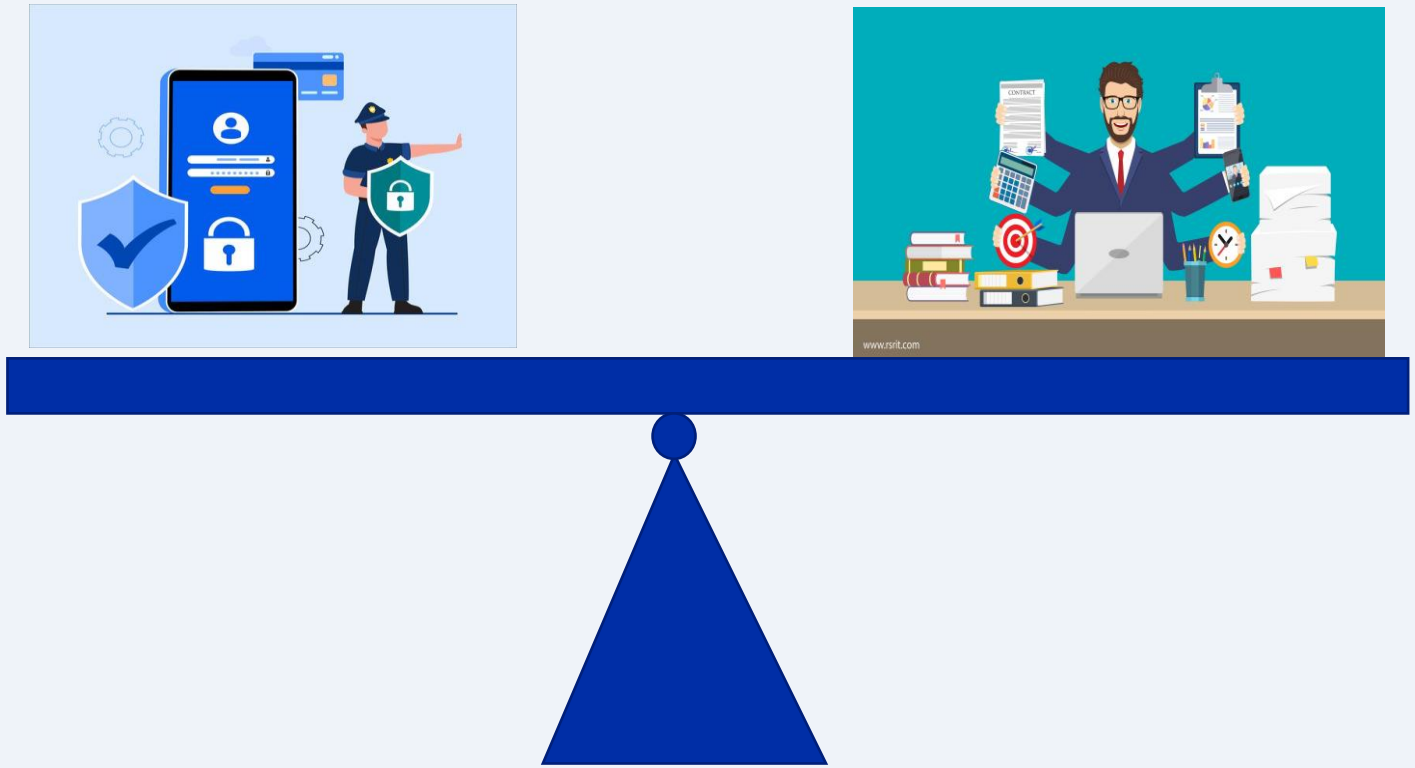
NIST
National Institute of Standards and Technology

Source: https://www.givainc.com/blog/index.cfm/2019/7/24/5-Key-Changes-Made-to-the-NIST-Cybersecurity-Framework-V11

Single Sign-On for SAP Systems

- Single Sign-On reduces the number of passwords by using Active Directory credentials instead of each SAP system having a different SAP password.
- Saves money and wasted time (time = money) on password resets
- More secure
  - Not having to keep a list of multiple passwords
  - Session is encrypted
  - Passwords are not transmitted over the network

Security vs Productivity



MFA – the pros and cons

CyberSafe

MFA – What is it?

Something You Know

******

Username, password, PIN or security questions

Something You Have

Smartphone, one-time passcode or Smart Card

Something You Are

Biometrics, like your fingerprint, retina scans or voice recognition

Popular MFA products: Microsoft Azure MFA , PingID, Okta, Duo, RSA SecurID

Microsoft MFA Survey

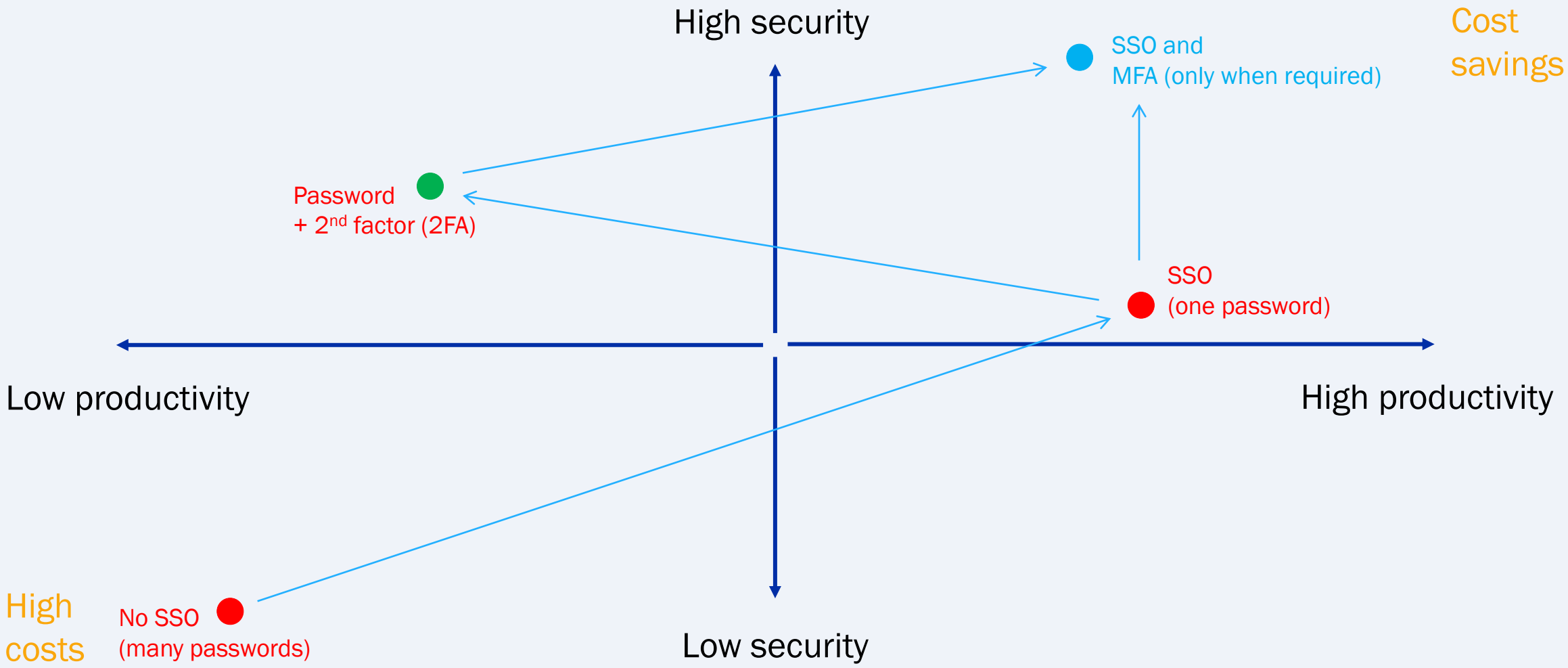
- 99.9% of compromised accounts did not use multi-factor authentication (MFA)
- Recent increase in uptake of MFA but mainly for VPN's (COVID-19 impact)
- Only 11% of all enterprise accounts use an MFA solution overall.

Source: https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/

How to use SSO with MFA

CyberSafe

Security, Cost, Authentication, Productivity



Protecting access to SAP systems and data

Using CyberSafe TrustBroker balances security and user productivity

Example 1:

- Use SSO by default, and
- Enforce MFA when the user accesses confidential or critical data

Example 2:

- Use SSO by default, and
- Enforce MFA when:
  - An administrator logs on, or
  - When an administrator performs an administrative task after logon

CyberSafe

Protecting access to SAP systems and data

Using CyberSafe TrustBroker balances security and user productivity

Authentication policy checks:

- SAP role assignment, e.g. does the user have an administrative role assigned
- Logon to systems that hold sensitive data, e.g. SAP Finance, HR system & personal data
- Logon from a certain network address range, e.g. Mobile workers
- When running specific SAP transactions, e.g. User administration transactions such as SU01
- When using Electronic Signatures, e.g. Approval of bank payments
- When accessing specific Dynpro fields and screens
    - Credit Card numbers being displayed
    - Payment amount > $x

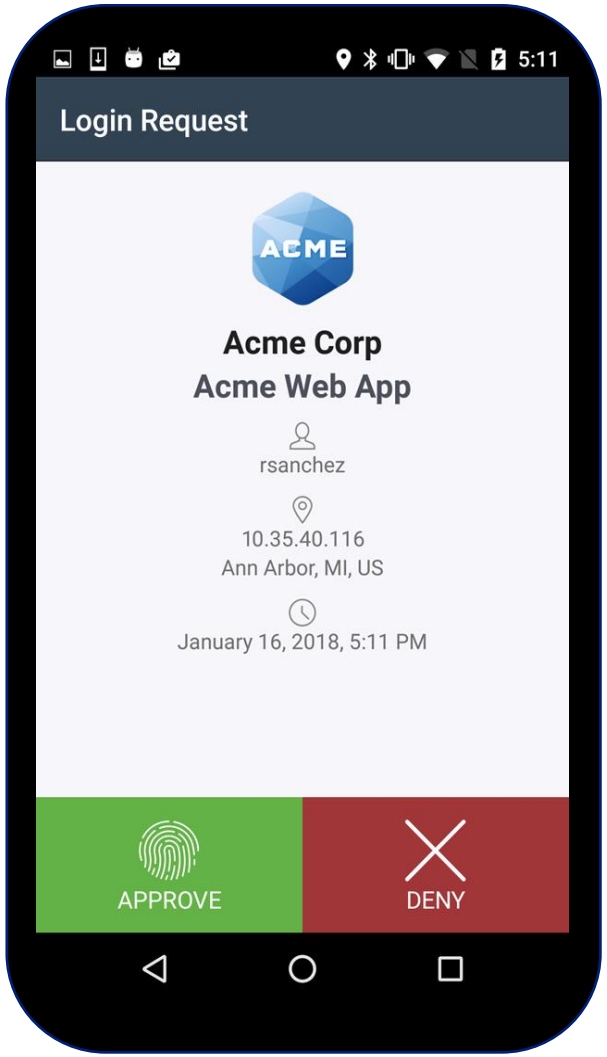
CyberSafe

A typical user experience with SAP GUI when using CyberSafe TrustBroker®

- Logon to workstation using **Active Directory** credentials (1st factor)
- Use SAP GUI or a web browser to logon to the SAP system (no credentials required, due to SSO)
- TrustBroker checks its authentication policy to determine if MFA is required. If it is, then:

  The user receives a push notification on their phone (2nd factor)

  The user presses the **APPROVE** button and uses their fingerprint
- Logon to the SAP system is successful



CyberSafe

Wrap Up

CyberSafe

Move from perimeter-based security towards Zero Trust

All resources are accessed in a secure manner regardless of location

Access Control is on a “need to know” basis and is strictly enforced

Never Trust and Always Verify

Apply MFA

Move towards a Passwordless future with SAP

- Come to our booth to talk to our experts, We can give a personalized demo to your company, and arrange a free proof-of-concept

Where to Find More Information

- Talk to our experts. Meet us on booth 1155 (Grand Ballroom)
- Register to try and win a Microsoft Xbox
- Web: https://CyberSafe.com/SAP

CyberSafe

Key Points to Take Home

- Do not rely on Trusted Zones
- Move towards Zero Trust
- Know where your sensitive data is stored
- Protect access using policies and SSO/MFA
- Balance Security with User Productivity
- Plan for a passwordless future

CyberSafe

Thank you! Any Questions?

John Mortimer

CyberSafe

John.Mortimer@cybersafe.com

www.cybersafe.com

Tel (44) 7766770261

Please remember to complete your session evaluation.

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.