A Security First Approach

Protecting Your Business in the Digital Economy

Gloria Lorenzo

Sr Director Oracle Product Development

Global Summit of Women 2022

Bangkok, 25 June 2022


Wallapop
Airbnb
Hangouts
STAR WARS
Yoda

FIREEYE™

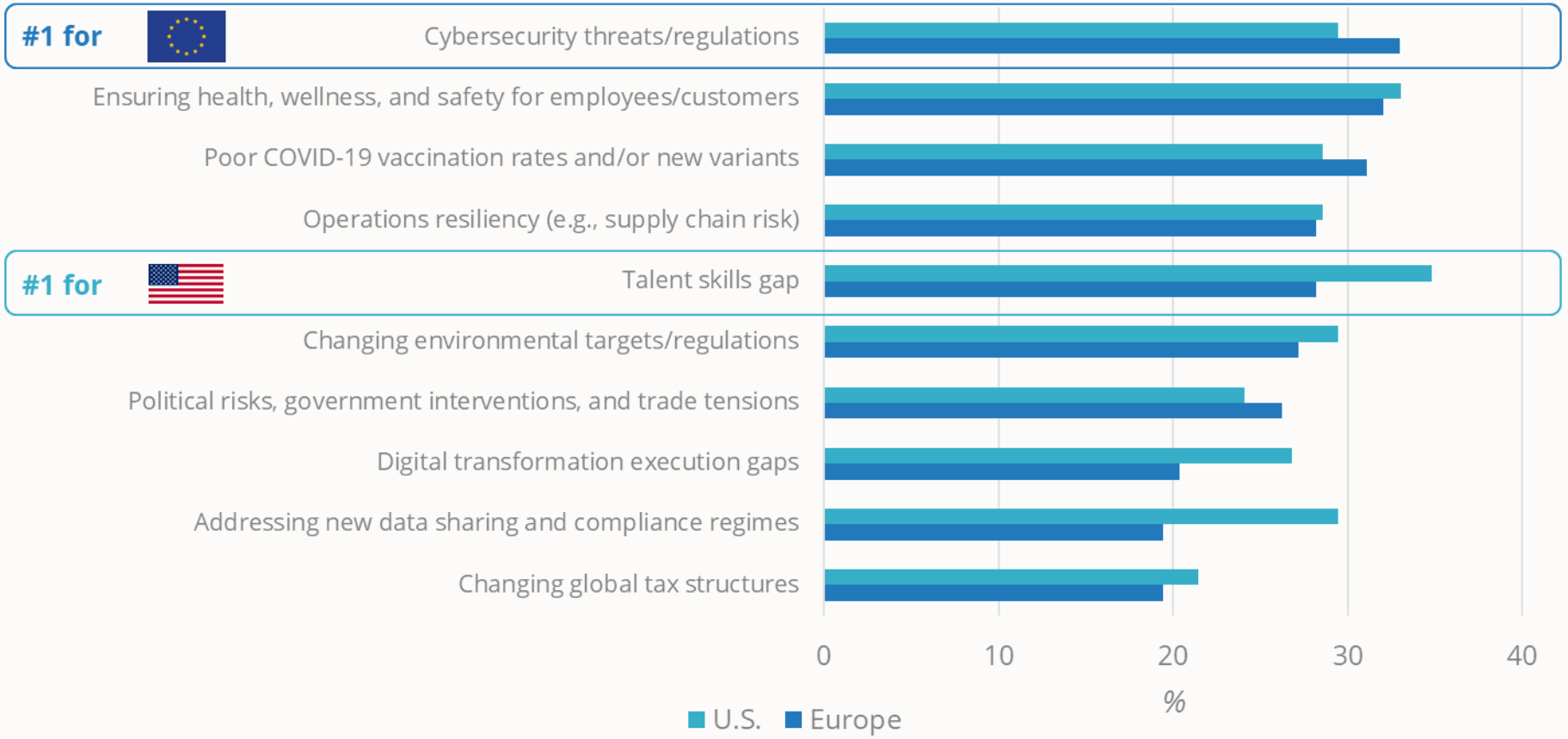
Today's cyber landscape has become a matter of 'when' not 'if' a cyber breach will affect your organization

Kevin Mandia – CEO. FireEye

Introduction to *The Executive's Breach Response Preparedness Playbook*

The pandemic is no longer seen as a top risk for European CEOs in 2022.

Of the following political, social, and economic risks, which three do you expect will have the greatest impact on your business in 2022?



The pandemic no longer seems to keep European CEOs awake at night. The biggest threat for 2022 is related to cybersecurity challenges and related regulations: first, because cybersecurity is a cornerstone of the European Commission's plans for a digital Europe, and second, because the rise in cyberattacks during the pandemic showed how crucial it is to invest in protecting more vulnerable organizations such as hospitals from such attacks. In the U.S., a talent skills gap is the greater threat for CEOs, linked with the Great Resignation movement and the related talent shortages.

This is reflected in fast spending growth: European IT security spending is expected grow 8.5% year over year, reaching €35 billion in 2022.

Sources: IDC's *Worldwide CEO Survey*, December 2021 (n = 103 European respondents); IDC's Worldwide Security Spending Guide, July 2021

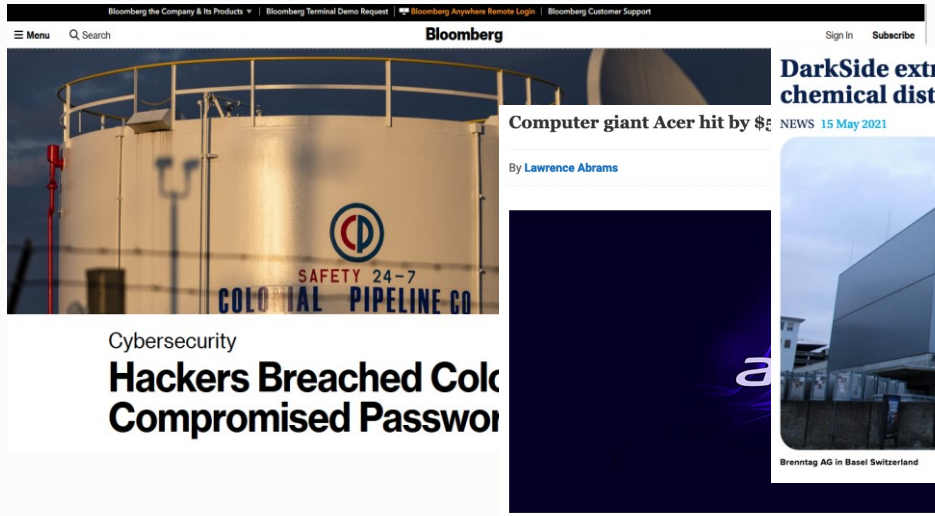
Threat Landscape as per ENISA

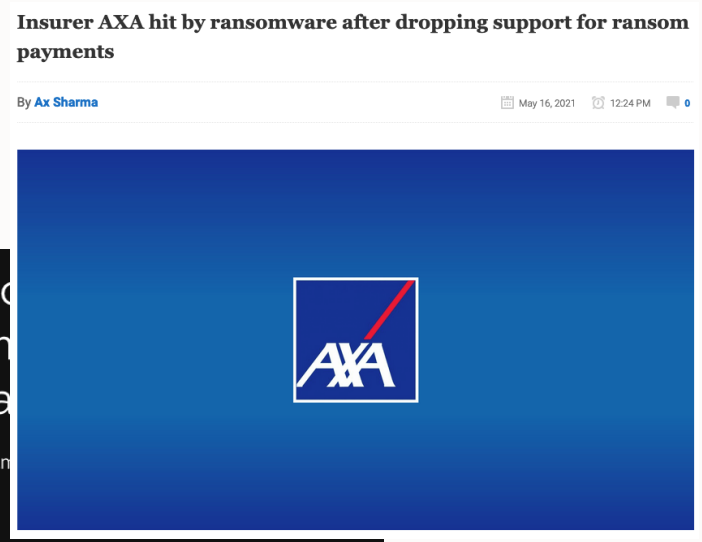
Top 9 (October 2021)

1. Ransomware
2. Malware
3. Cryptojacking
4. E-mail related threats
5. Threats against data (this category encompasses data breaches/leaks)
6. Threats against availability and integrity
7. Disinformation – misinformation
8. Non-malicious threats (mostly human errors and system misconfigurations)
9. Supply-chain attacks

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Ransomware and data breaches are a major problem





Over 4,000 attacks daily
(source: FBI)

US organizations lost more than
$7.5 billion in 2019
(source: Emsisoft)

19-day average downtime
(source: Coveware)

Average total cost of a data breach: $ 3.86M

Cost per lost record: $ 150

Average size of a data breach:
25,575 records

Average total cost of remediating $1.85M
(source: Sophos)

Source: https://www.blackfog.com/the-state-of-ransomware-in-2021/#May

Ransomware: Main actions to reduce risks

Ransomware risk and process Assessment

Vulnerability Management

- Authentication
- Identity management
- Key vaulting

Data Protection

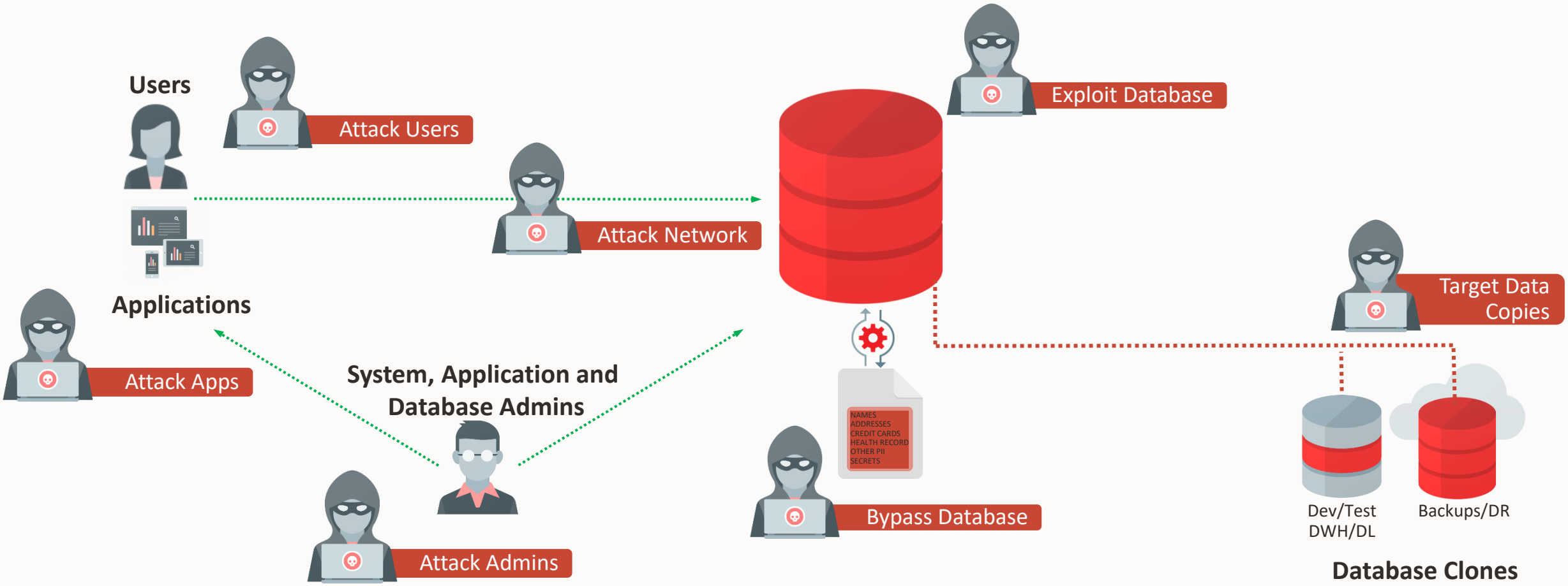
- Multiple, offline and vaulted backup copies
- Immutable backup
- Access control
- Effective and fast recoveries
- Reducing data loss gap
- Database Encryption

Maintain & Monitor

- Maintenance
- Patching
- Auditing

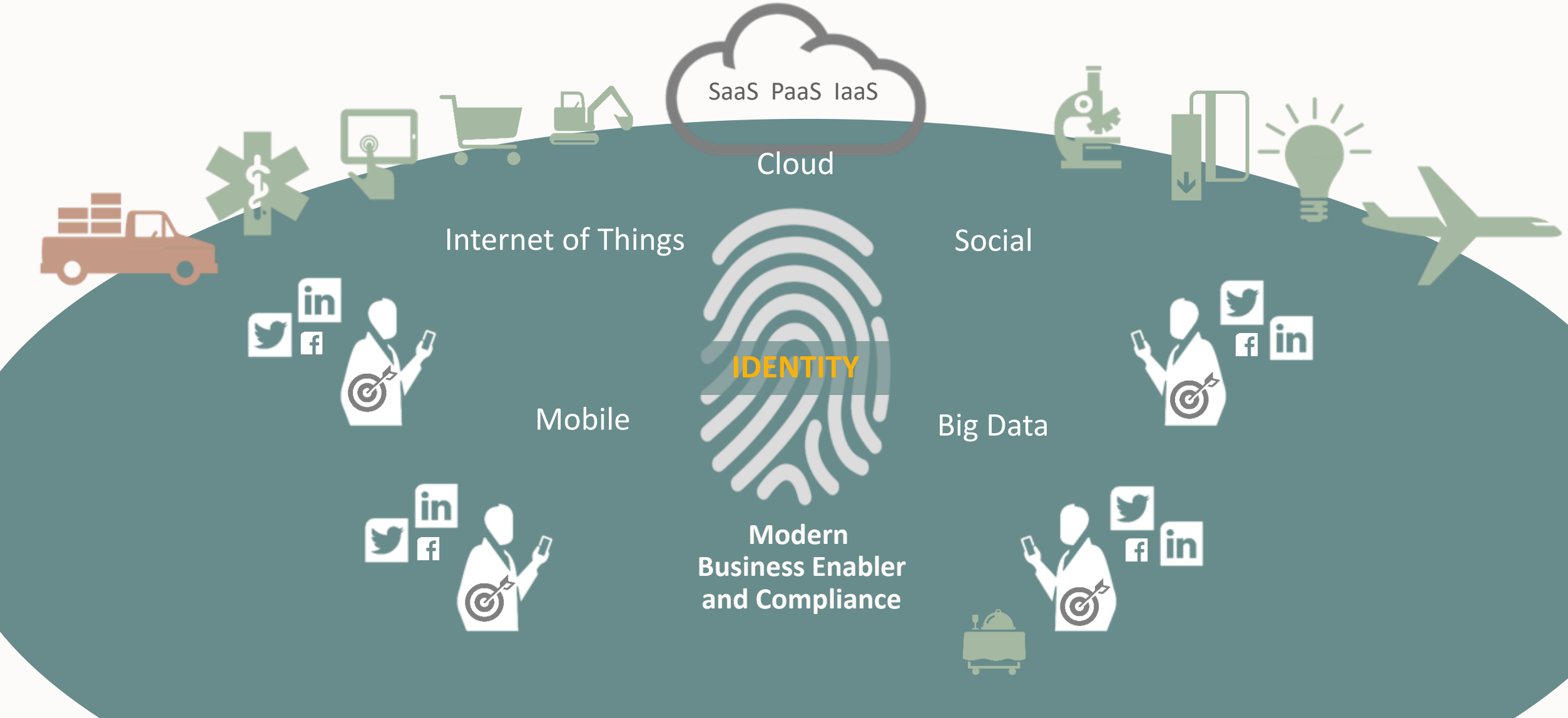
Security starts with your data…

How Do “bad guys” steal our Data?



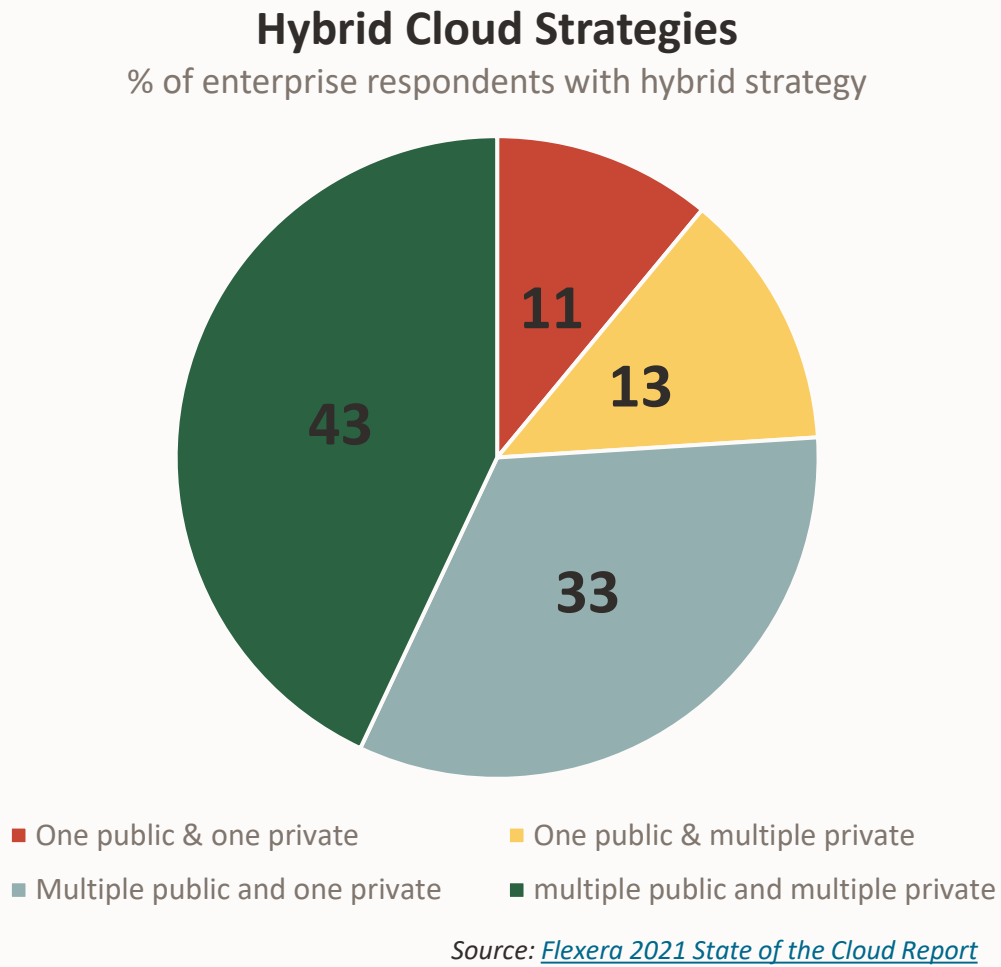
Identity is Crucial for the Hybrid Enterprise

Zero trust security is driving identity as a key resource



Security paradigm shift – Where are my assets?

Can organizations still be secure?



Source: Flexera 2021 State of the Cloud Report

#1

Shared responsibility for security

Can cause confusion over roles and responsibilities

Devices & Things

Users

Content

Applications

Infrastructure

"Through 2025, more than 99% of cloud breaches will have a root cause of **preventable misconfigurations or mistakes by end users**"

Gartner

(Gartner®, Hype Cycle™ for Cloud Security, 2022, Tom Croll, Jay Heiser, 27 July 2022.
GARTNER and HYPE CYCLE are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission.
All rights reserved.)

#2

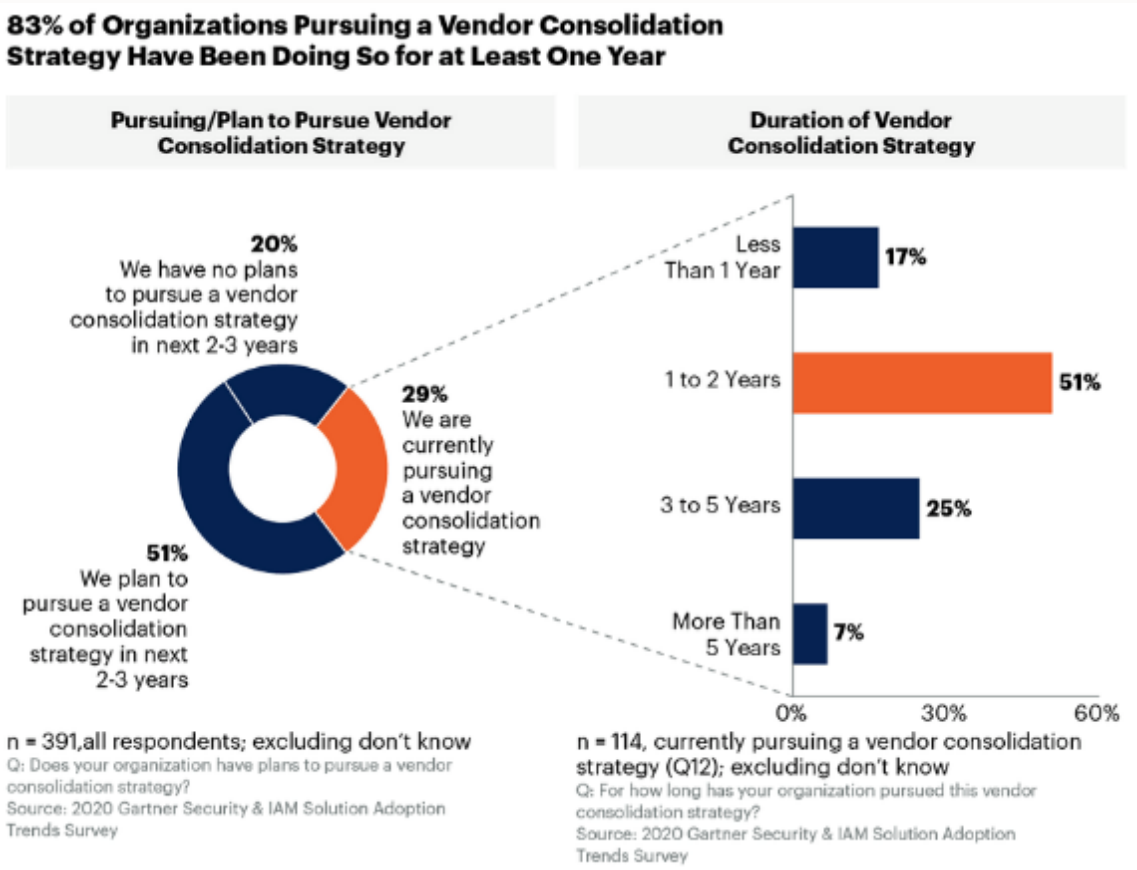
What Does it take to Secure your Assets Today?

Too Complex…

78 percent of organizations use more than 50 discrete cybersecurity products to address security issues

37 percent use more than 100 cybersecurity products.

- The large number of security products used by organizations drives up complexity and integration costs.
- Organizations want vendor consolidation to simplify operations and reduce overall costs.



Sources:

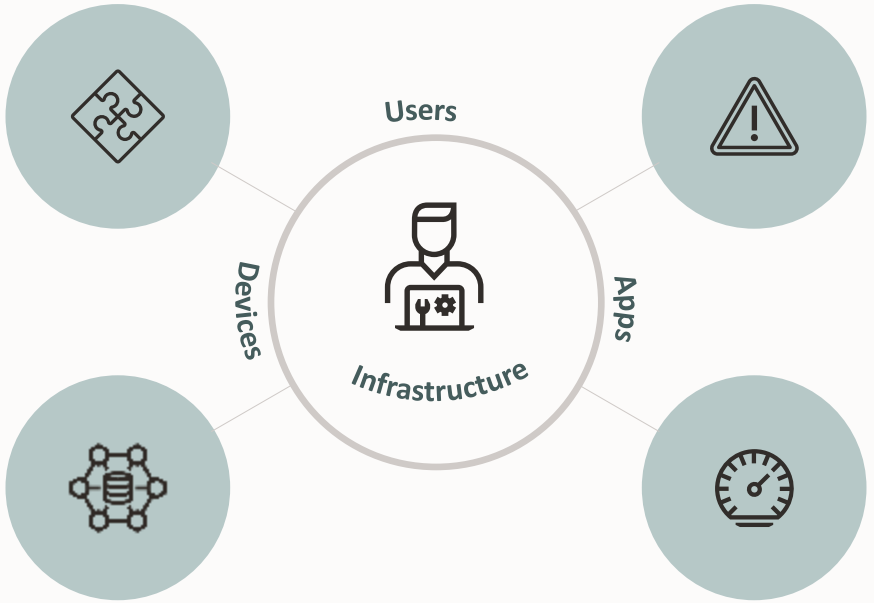
Oracle and KPMG Cloud Threat Report 2020

Gartner: Top Security and Risk Management Trends 2021

Will More Tools Result in Better Security?

Integration
A lot of security tools!
Many different APIs

Interoperability
Customers have to put tools together themselves



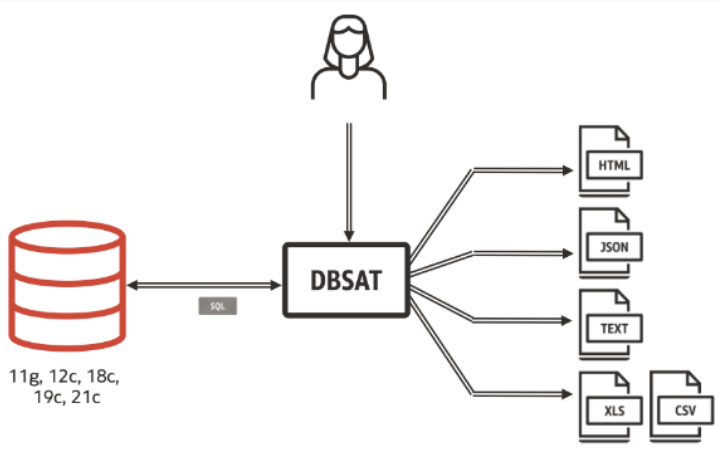
Ease-of-Use
No real instructions
Experts required

Monitoring
Multiple dashboards & workflows
Many vendors

Defense in Depth

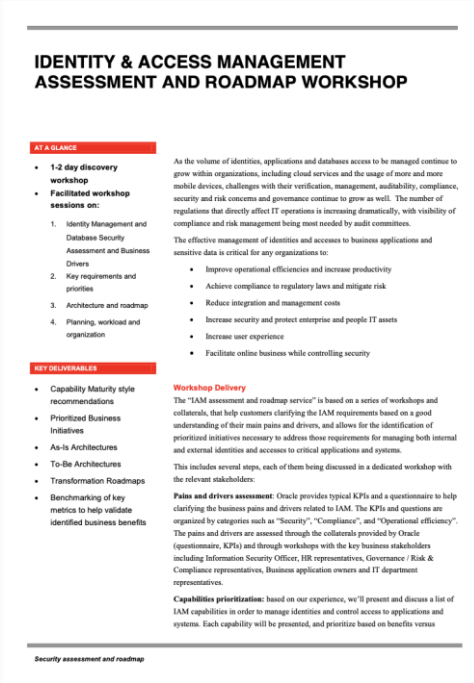
Assessing Your Security

Database Assessment



Data Safe

IAM Assessment



IDENTITY & ACCESS MANAGEMENT ASSESSMENT AND ROADMAP WORKSHOP

AT A GLANCE

- **1-2 day discovery workshop**
- **Facilitated workshop sessions on:**
  1. Identity Management and Database Security Assessment and Business Drivers
  2. Key requirements and priorities
  3. Architecture and roadmap
  4. Planning, workload and organization

KEY DELIVERABLES

- Capability Maturity style recommendations
- Prioritized Business Initiatives
- As-Is Architectures
- To-Be Architectures
- Transformation Roadmaps
- Benchmarking of key metrics to help validate identified business benefits

As the volume of identities, applications and databases access to be managed continue to grow within organizations, including cloud services and the usage of more and more mobile devices, challenges with their verification, management, auditability, compliance, security and risk concerns and governance continue to grow as well. The number of regulations that directly affect IT operations is increasing dramatically, with visibility of compliance and risk management being most needed by audit committees.

The effective management of identities and accesses to business applications and sensitive data is critical for any organizations to:

- Improve operational efficiencies and increase productivity
- Achieve compliance to regulatory laws and mitigate risk
- Reduce integration and management costs
- Increase security and protect enterprise and people IT assets
- Increase user experience
- Facilitate online business while controlling security

Workshop Delivery

The "IAM assessment and roadmap service" is based on a series of workshops and collaterals, that help customers clarifying the IAM requirements based on a good understanding of their main pains and drivers, and allows for the identification of prioritized initiatives necessary to address those requirements for managing both internal and external identities and accesses to critical applications and systems.

This includes several steps, each of them being discussed in a dedicated workshop with the relevant stakeholders:

Pains and drivers assessment: Oracle provides typical KPIs and a questionnaire to help clarifying the business pains and drivers related to IAM. The KPIs and questions are organized by categories such as "Security", "Compliance", and "Operational efficiency". The pains and drivers are assessed through the collaterals provided by Oracle (questionnaire, KPIs) and through workshops with the key business stakeholders including Information Security Officer, HR representatives, Governance / Risk & Compliance representatives, Business application owners and IT department representatives.

Capabilities prioritization: based on our experience, we'll present and discuss a list of IAM capabilities in order to manage identities and control access to applications and systems. Each capability will be presented, and prioritize based on benefits versus

Security assessment and roadmap

- Assess your current state
- Develop a mitigation strategy based on findings and company strategy
- Identify incremental and ongoing steps to reduce risk and improve security

Thank you!

Gloria Lorenzo

Twitter: @glorenjor

LinkedIn: https://www.linkedin.com/in/gloria-lorenzo-7273791/