



Keynote
**2024 Global Mobile Threat Report: A
Topical
Analysis of Mobile Threat Data from the
Field**

Geert NOBELS
Tribe Leader EMEA
CISSP CCSP CISM CISA CDPSE CCAK CCSK

What is the first device your user used for work today?

How confident are you they:

- Will update their OS in time?
- Will not jailbreak / root their device?
- Will not install apps that have privacy or data loss concerns?
- Will not click or scan phishing links?
- Will not connect to unsafe networks?

How confident are you they will be cyber hygiene?

A call for mobile cyber hygiene based on our 2024 threat data!

-Question-





A QUIET REVOLUTION IS UPON US

A digital surge has catalyzed
mobile behavior...

catapulting companies toward
mobile-powered business models



PRODUCTIVITY: MOBILE *IS* THE MODERN WORKPLACE

To get **work done** anywhere/
anytime, employees are:

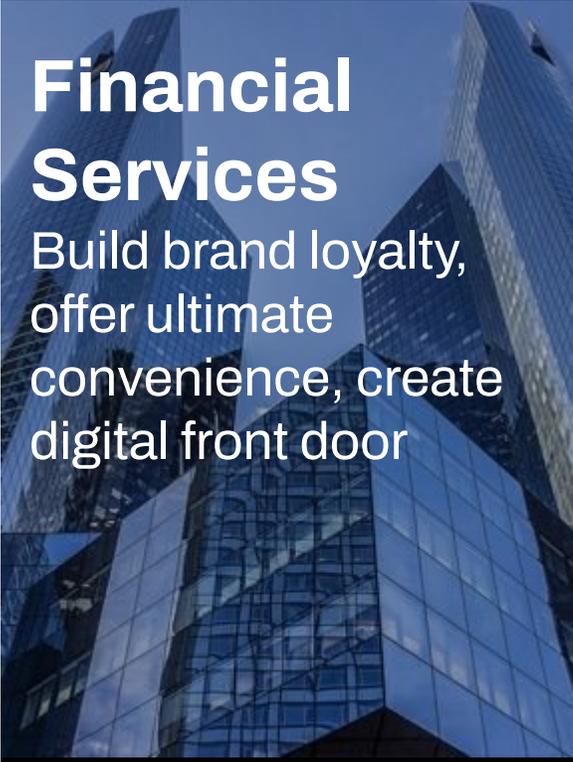
Adopting an
explosion of
mobile apps

Conducting
more mobile
transactions

Tightly
collaborating
with more people

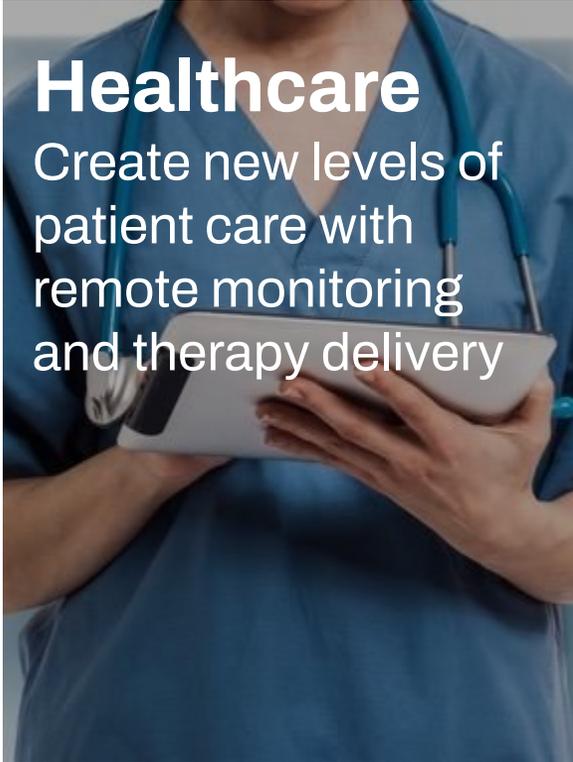
Accessing
higher volumes
of **data**

Opening up a new world of **mobile-powered opportunities**



Financial Services

Build brand loyalty, offer ultimate convenience, create digital front door



Healthcare

Create new levels of patient care with remote monitoring and therapy delivery



Automotive

Offer consumers increased control, monitor safety and automotive efficiency

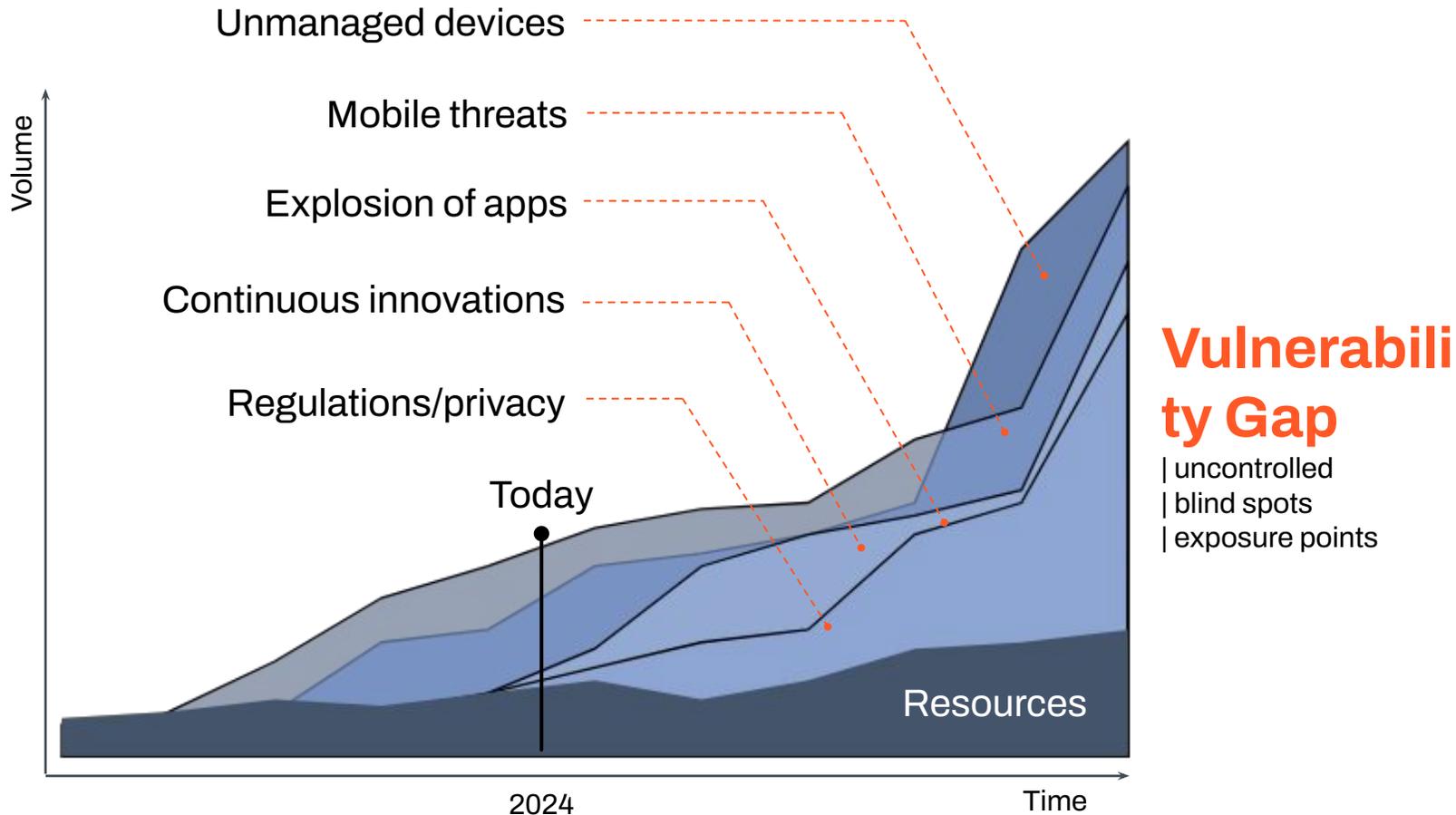


Public Sector

Engage citizens, enable mobile participation in city planning; provide convenient access to payments, utilities and more

RISK MOVES TO THE EDGE

The escalating **Vulnerability Gap**



Creating negative consequences

BRAND IMPACT

46%

suffered reputational damage

FINANCIAL IMPACT

\$29B

digital fraud from mobile

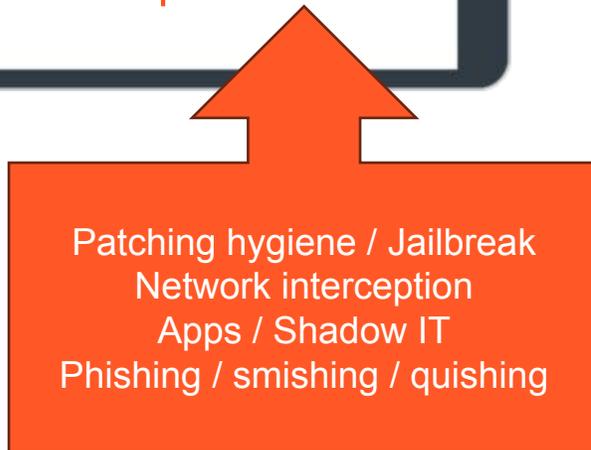
BOARD-LEVEL PRIORITY

88%

view cyber risk as business risk

Threat visibility for mobile devices

MOBILE CYBER HYGIENE



Device

65% of enterprise devices running an OS with **CRITICAL** vulnerabilities



Network

1:5

One in five enterprise mobile devices experienced a network attack



Applications

144,000

New mobile malware signatures per month



Phishing

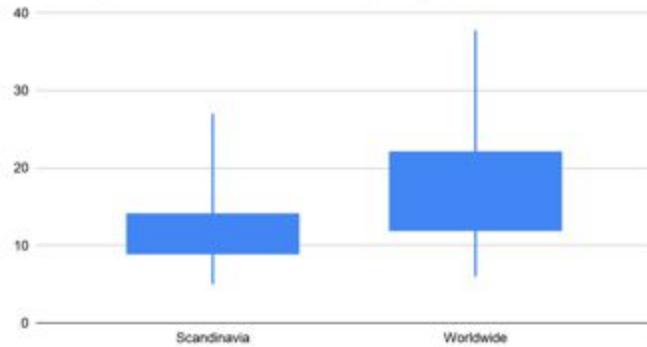
90% of breaches start with phishing;
60% of emails read on mobile

Innovation & attacks make mobile cyber hygiene challenging

- **OS challenges (demo)**
 - Increased **update** cycle of mobile OS
 - Availability and ease of use of **jailbreak** tools
- **Connectivity**
 - Lack of connectivity when **roaming**, makes network security challenging (eg. **Olympics**)
- **App stores (demo)**
 - **Third party app stores** (Digital Markets Act)
 - Mobile **app code quality** / **AI** / SDK / libraries / local frameworks / code re-use (>50%)
- **Phishing (demo)**
 - **Phishing** links in PDF to bypass security controls
 - SMS links unreadable for the user, leading to **smishing**
 - QR codes even worse, leading to **quishing**
- **Innovations versus security (demo)**
 - **Shortcuts** exploited to manipulate the device

PATCHING HYGIENE / JAILBREAK

Time to update device from release (in days)



**% tampered
not rooted/jailbroken**

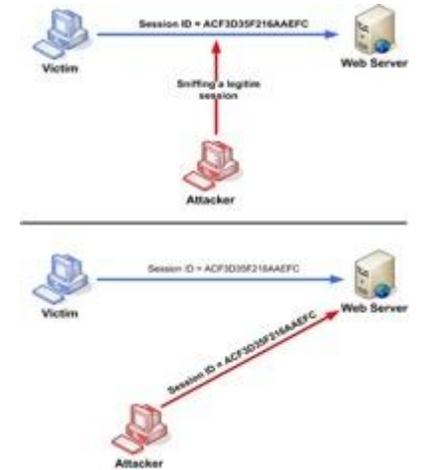
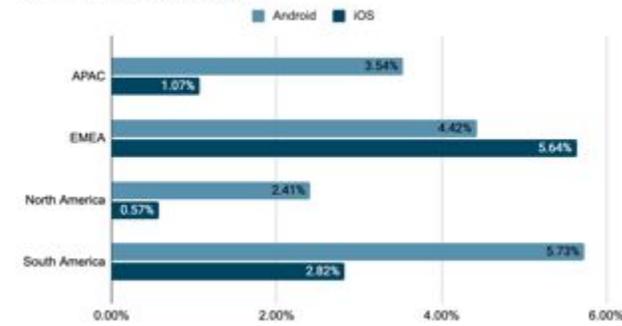
51%

41%

Total 43%

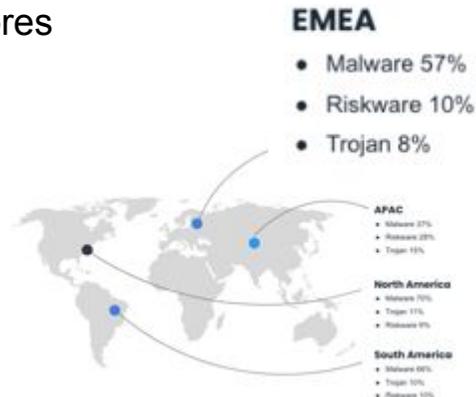
NETWORK INTERCEPTION

Network Attacks by Region



APPS / SHADOW IT

- Sideloaded / 3rd party App stores
- Malware 2023



PHISHING/ SMISHING / QUIISHING

Emails have an average click rate of **2%**, whereas SMS click rates range between **5.9%** and **14.6%**.

The average user is **3 to 7** times more likely to fall for an SMS phishing attack

NIS2
Directive



a Mobile-First Security Strategy



National Cyber
Security Centre
a part of GCHQ

1

Prioritize risk at the edge: secure the mobile-powered business reality, across all devices and apps, any platform

2

Operate in a known state: complete visibility of your mobile ecosystem and risk level, automatically assess vulnerabilities, never throttle productivity - measurable, auditable and insurable

3

Step-up detection and response: detect and prioritize anomalies, contextual threat response, resolve vulnerabilities and incidents proactively, embed security across device and application lifecycle for tamper-proof/threat-aware mobile experiences

4

Start the autonomous journey: dynamically respond to threats and ever-changing mobile ecosystem, automatically isolate compromised devices/ untrusted environments, scale a proactive security posture, build resilience

5

Never break the law: govern compliance, stay ahead of global regulations, data sovereignty, and privacy regulations while respecting work/life boundaries

Tuesday	Wednesday	Topic & Meeting Room
04:00 PM - 04:45 PM	09:00 AM - 09:45 AM	SIA Session 3: Zimperium Your Data Is mobile. Is Your Security? Studio 4 Join this session with Zimperium to learn about the latest mobile threats and how Zimperium protects mobile endpoints and apps so they can access enterprise data securely. You will also learn on how Zimperium and Trellix work together to create a unified orchestration layer for seamless customer experience.

SIA Session 3: Zimperium Studio 4

Your data is mobile. Is your security?

Marcos REGIDOR
Director Technical Sales

Geert NOBELS
Tribe Leader EMEA
CISSP CCSP CISM CISA CDPSE CCAK CCSK