Security and privacy for information systems

Mikko Karikytö
Chief Product Security Officer &
Head of Product Security

Dario Casella
Head of Product Privacy

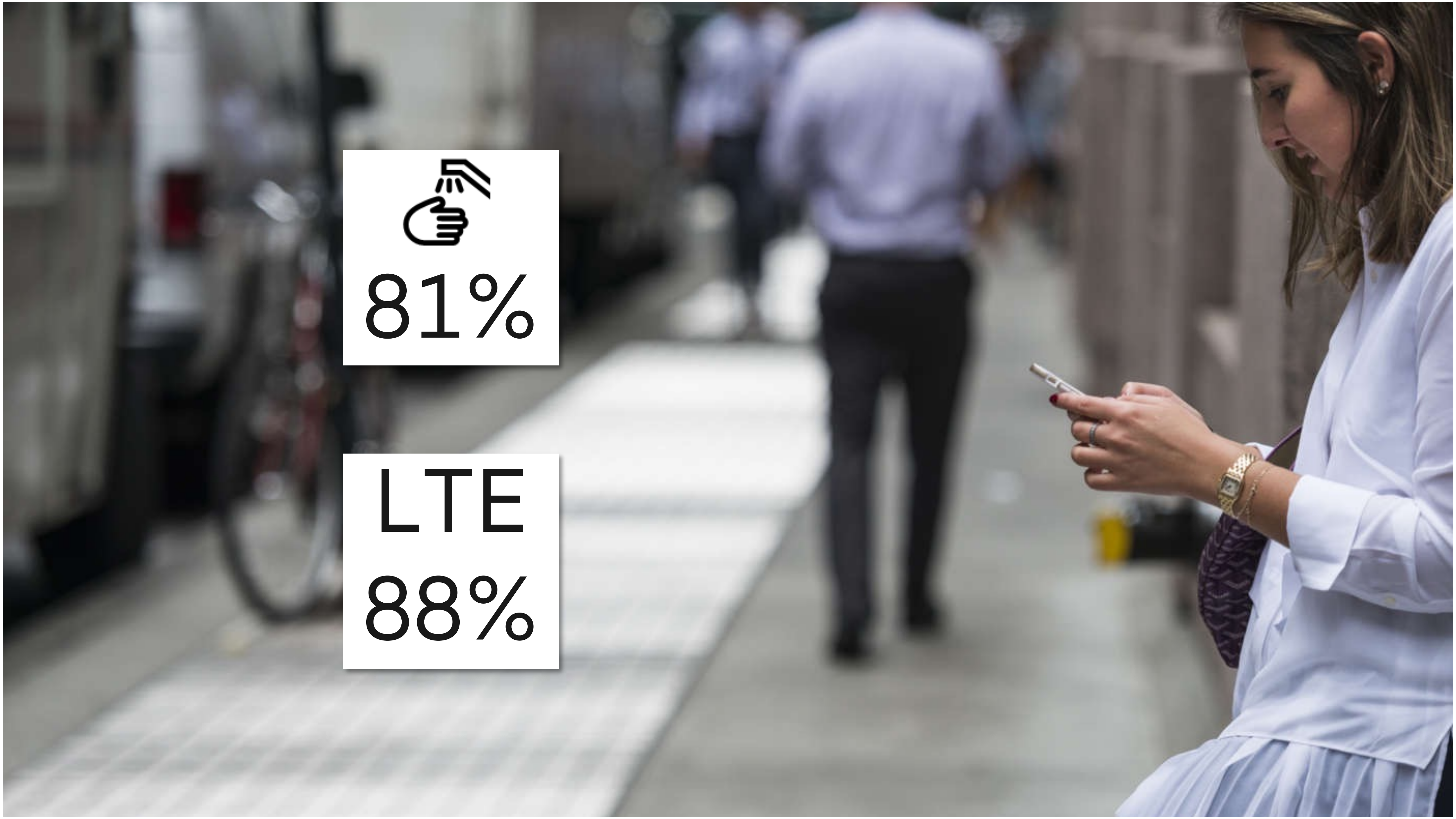
Ericsson

https://twitter.com/_mg_/status/1054929638621757441

Content today

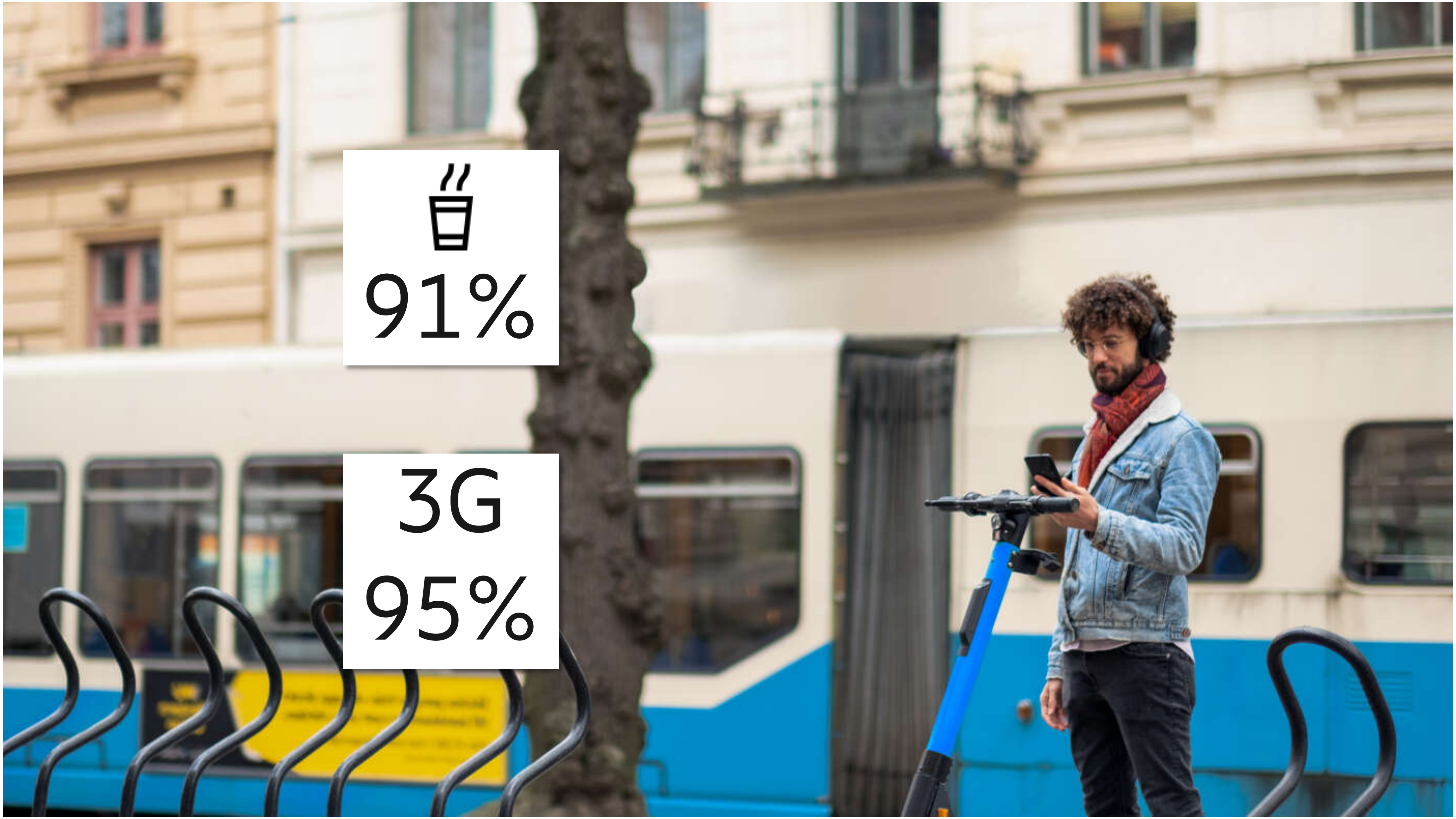
- Our background and relation to security and privacy
- What security consists of?
- What does privacy of information systems mean?
- What should you *do, or know* to ask for?

Mobile network, its role in society and relation to security & privacy



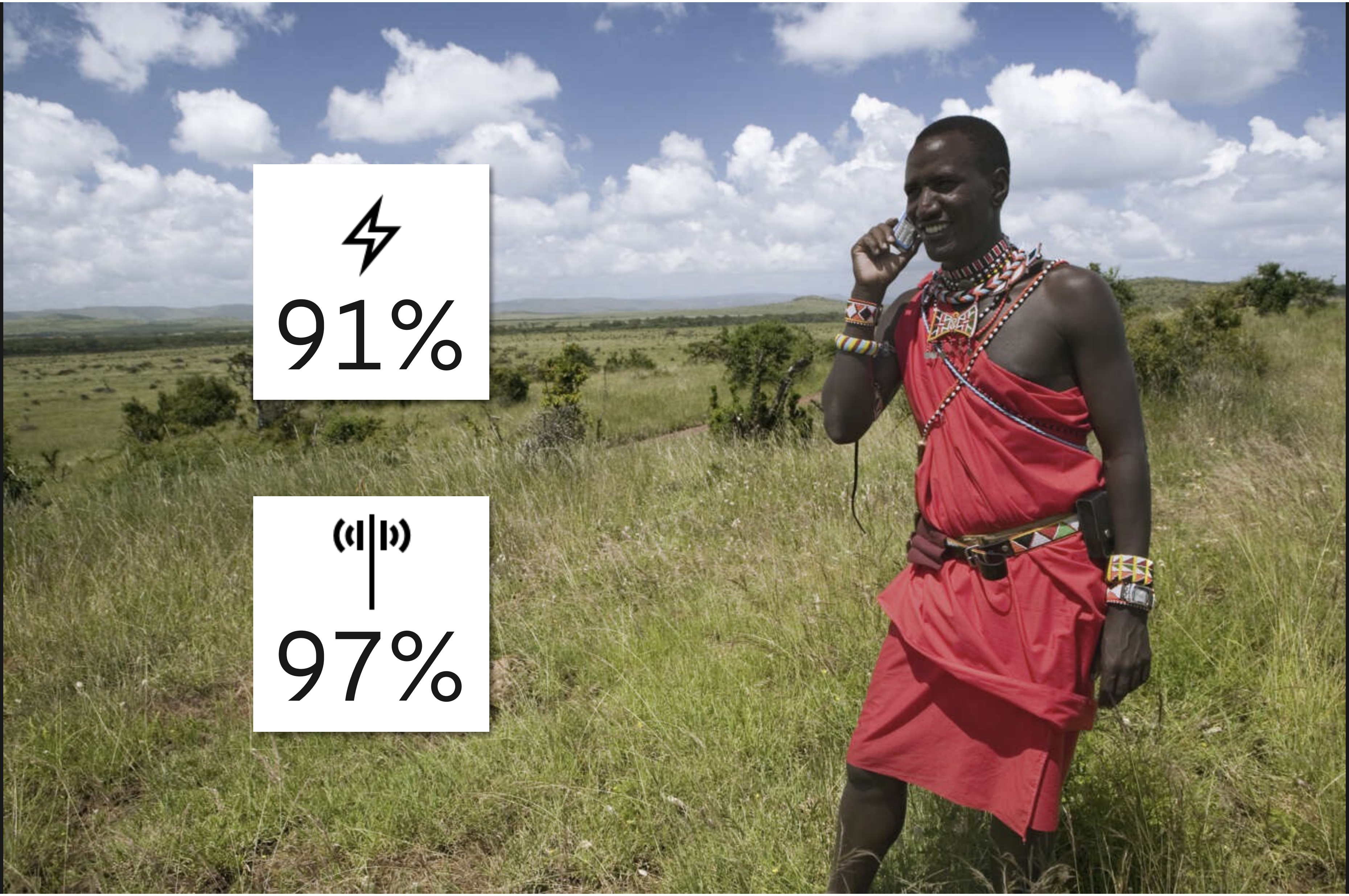
81%

LTE
88%



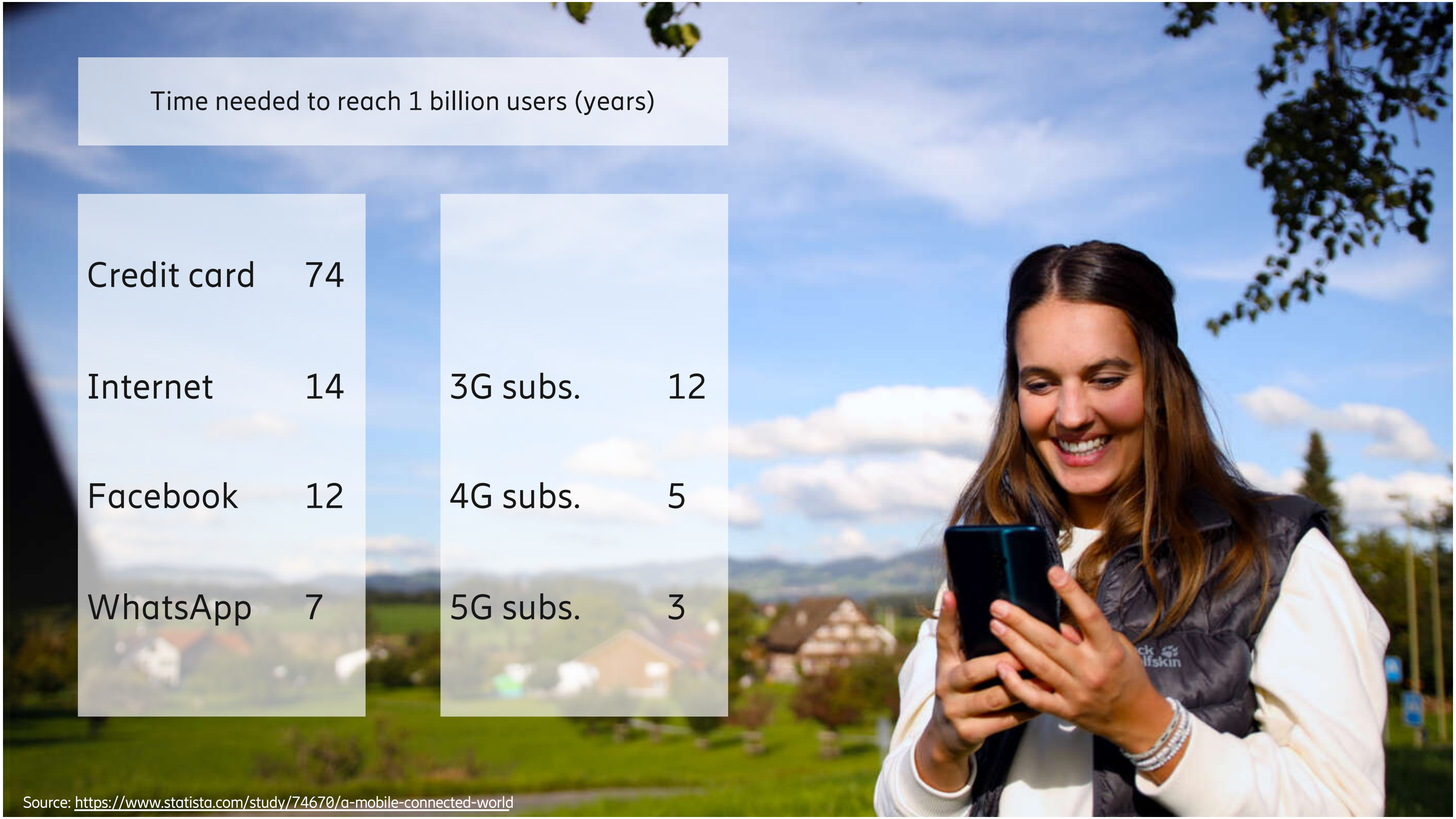
☕ 91%

3G 95%



91%

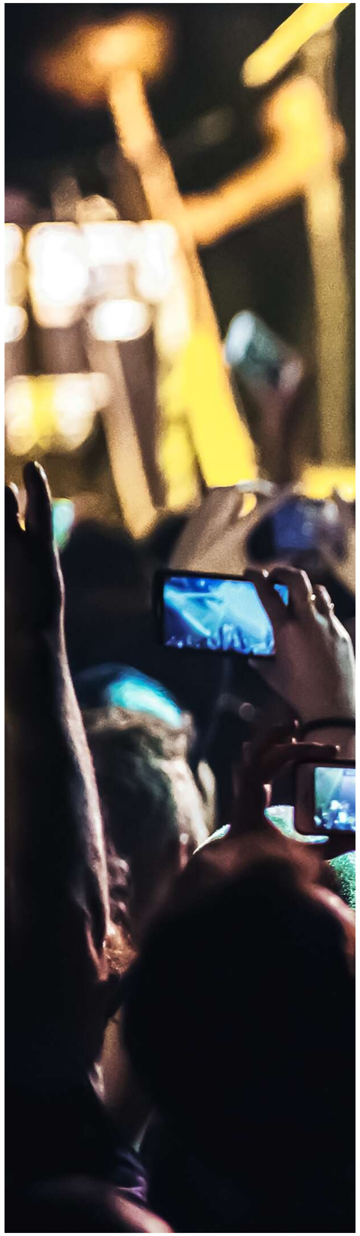
97%



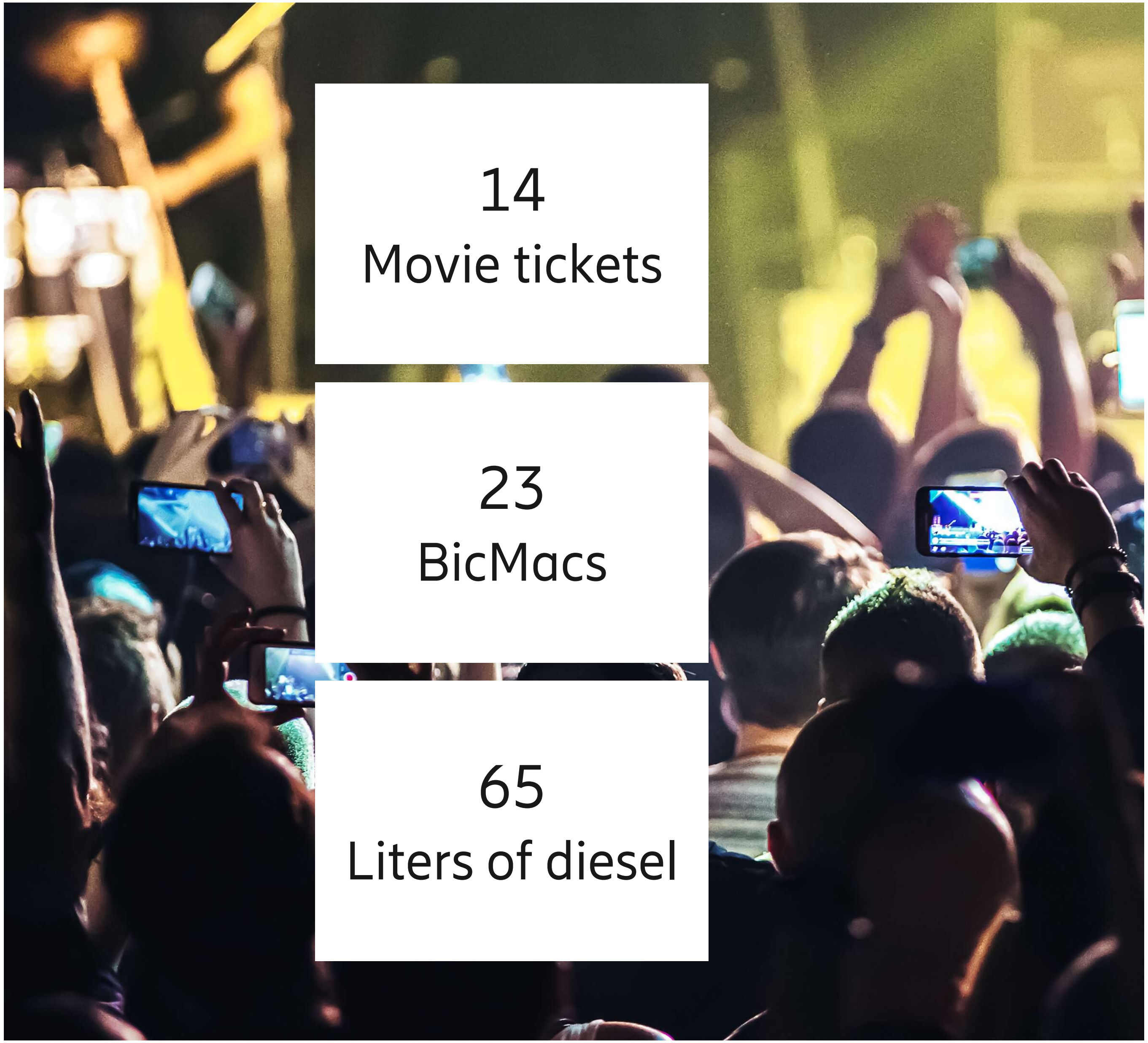
Time needed to reach 1 billion users (years)

Credit card	74		
Internet	14	3G subs.	12
Facebook	12	4G subs.	5
WhatsApp	7	5G subs.	3

Source: https://www.statista.com/study/74670/a-mobile-connected-world



10 years ago

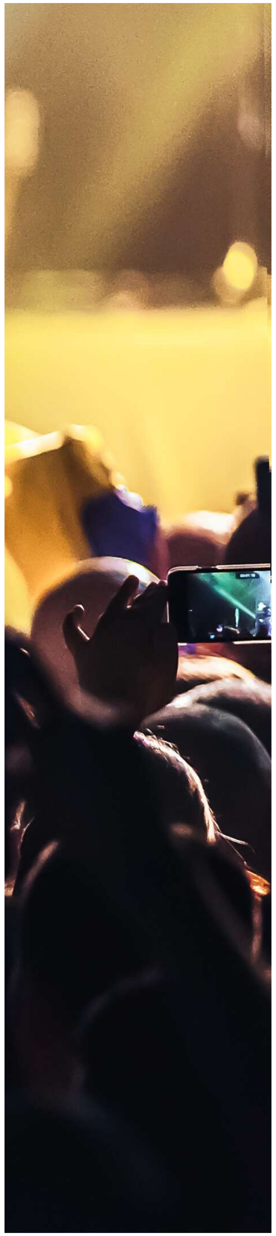


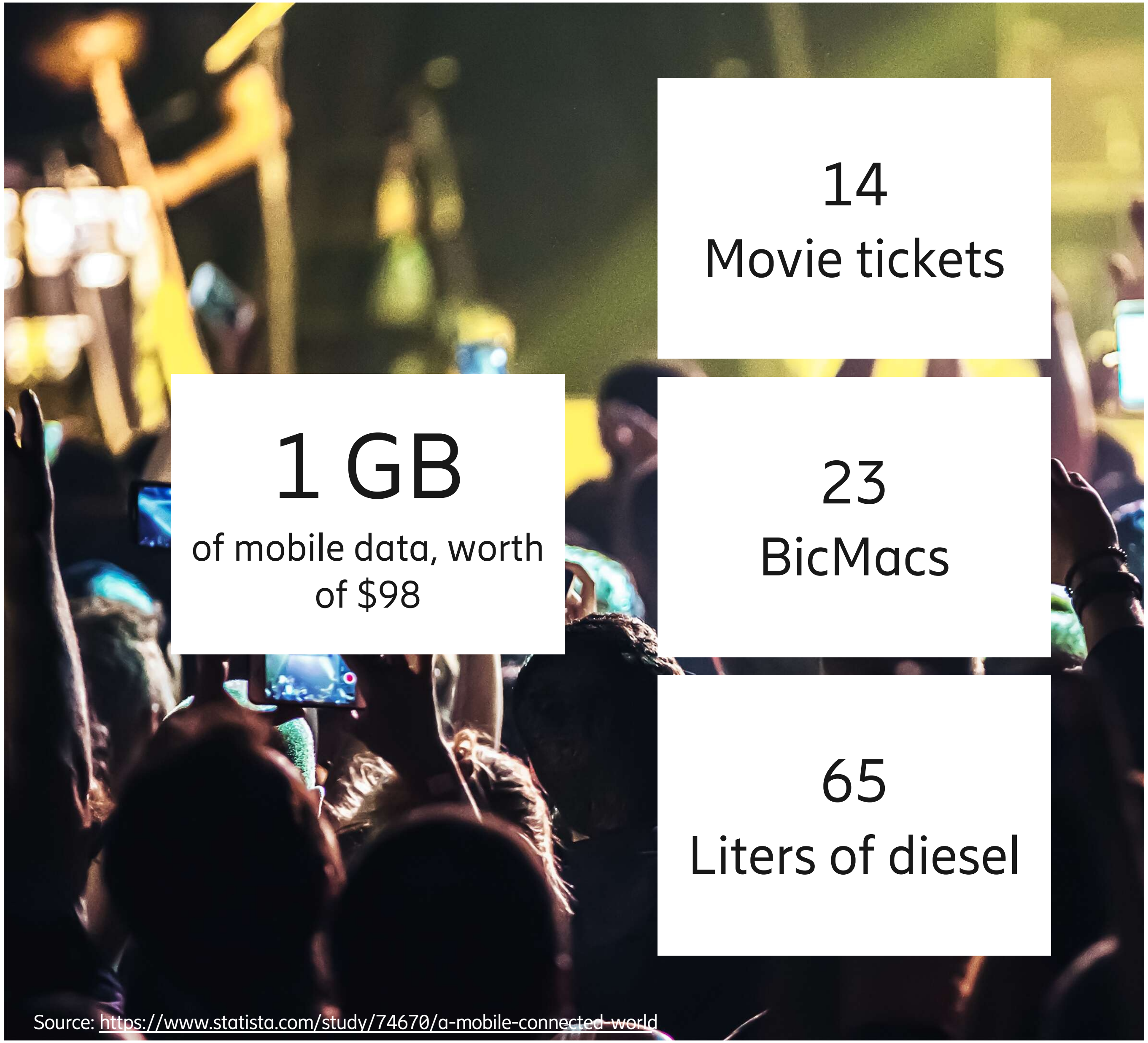
14
Movie tickets

23
BicMacs

65
Liters of diesel

12 years ago





1 GB

of mobile data, worth of $98

14

Movie tickets

23

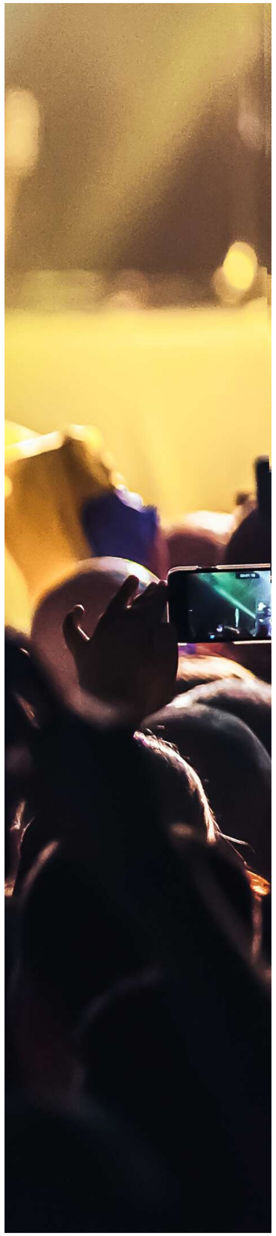
BicMacs

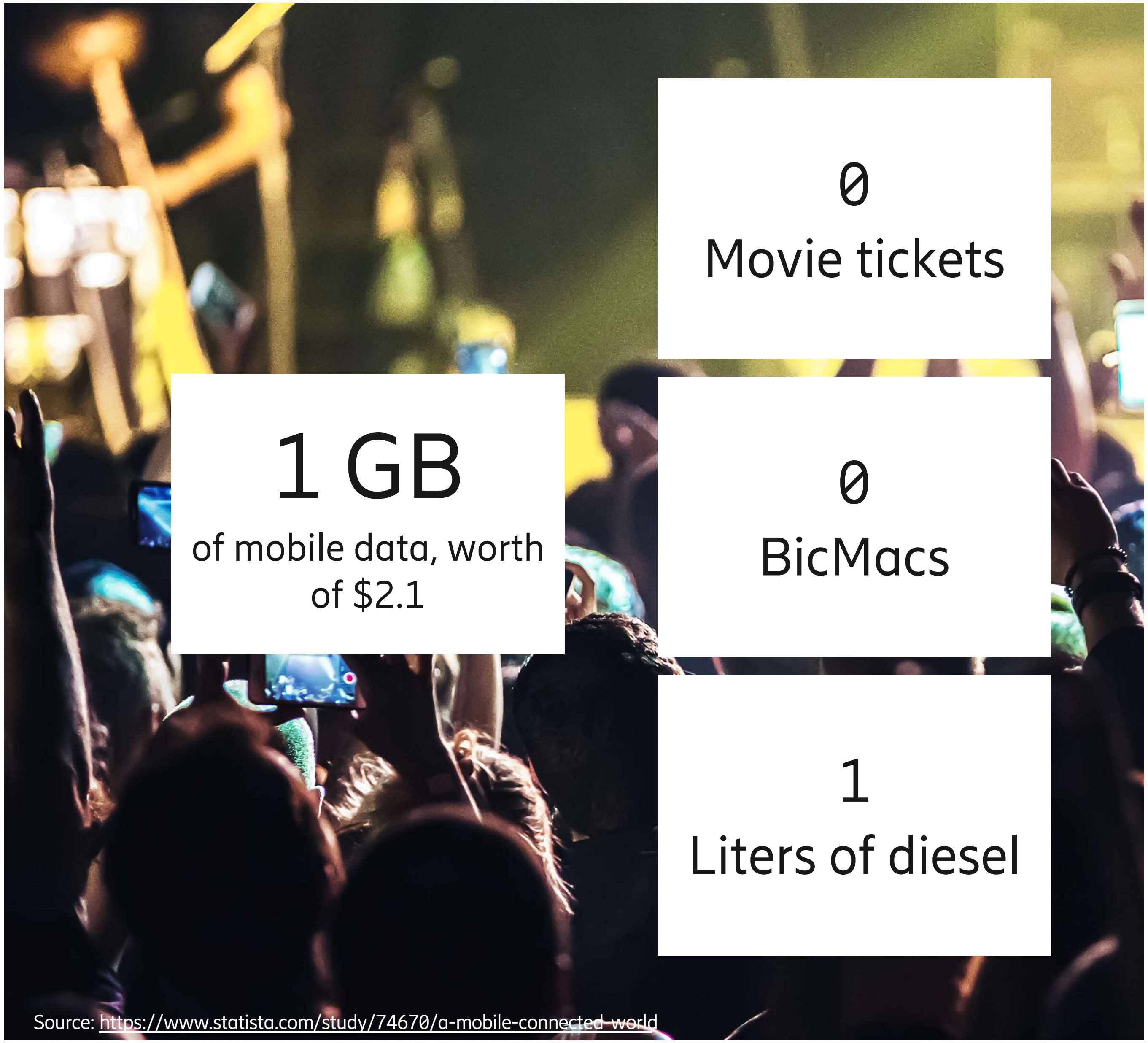
65

Liters of diesel

Source: https://www.statista.com/study/74670/a-mobile-connected-world

12 years ago





1 GB

of mobile data, worth of $2.1

0

Movie tickets

0

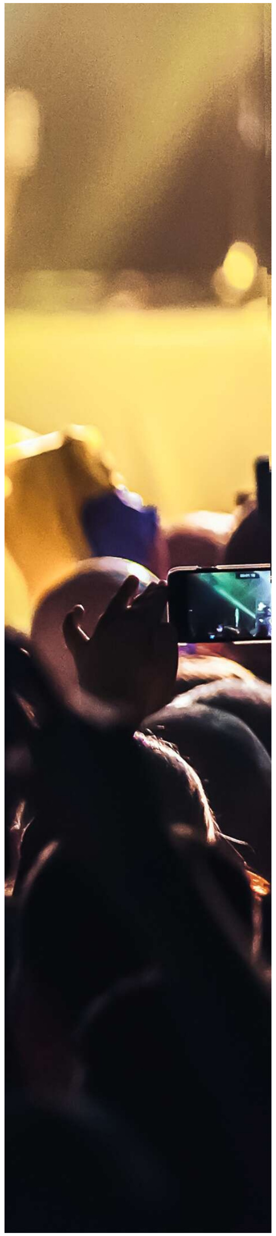
BicMacs

1

Liters of diesel

Source: https://www.statista.com/study/74670/a-mobile-connected-world

Today



A child speaks on the phone as he says goodbye to a relative looking out the window of a train carriage waiting to leave for western Ukraine at the railway station in Kramatorsk, Ukraine on March 2, 2022. | Andriy Andriyenko/AP Photo

https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487

Mobile industry has been shaped through shared innovation

700

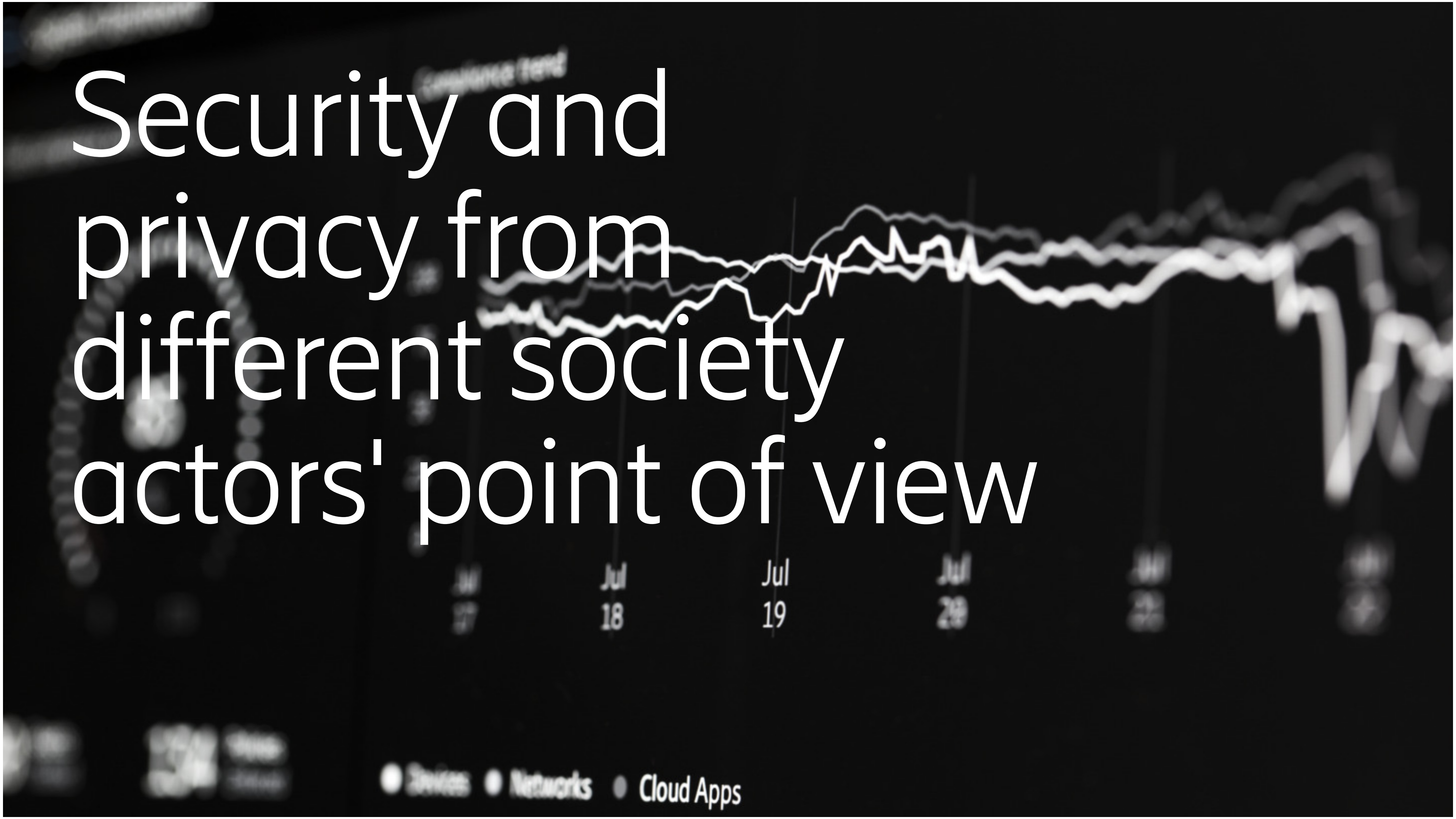
Companies collaborate today

>100

Open interfaces

One global standard leveraged by large ecosystem enabling standard based innovation in mobile communication devices and network equipment.

Security and privacy from different society actors' point of view



130
130

For individual:

- Feeling of safety, security and privacy

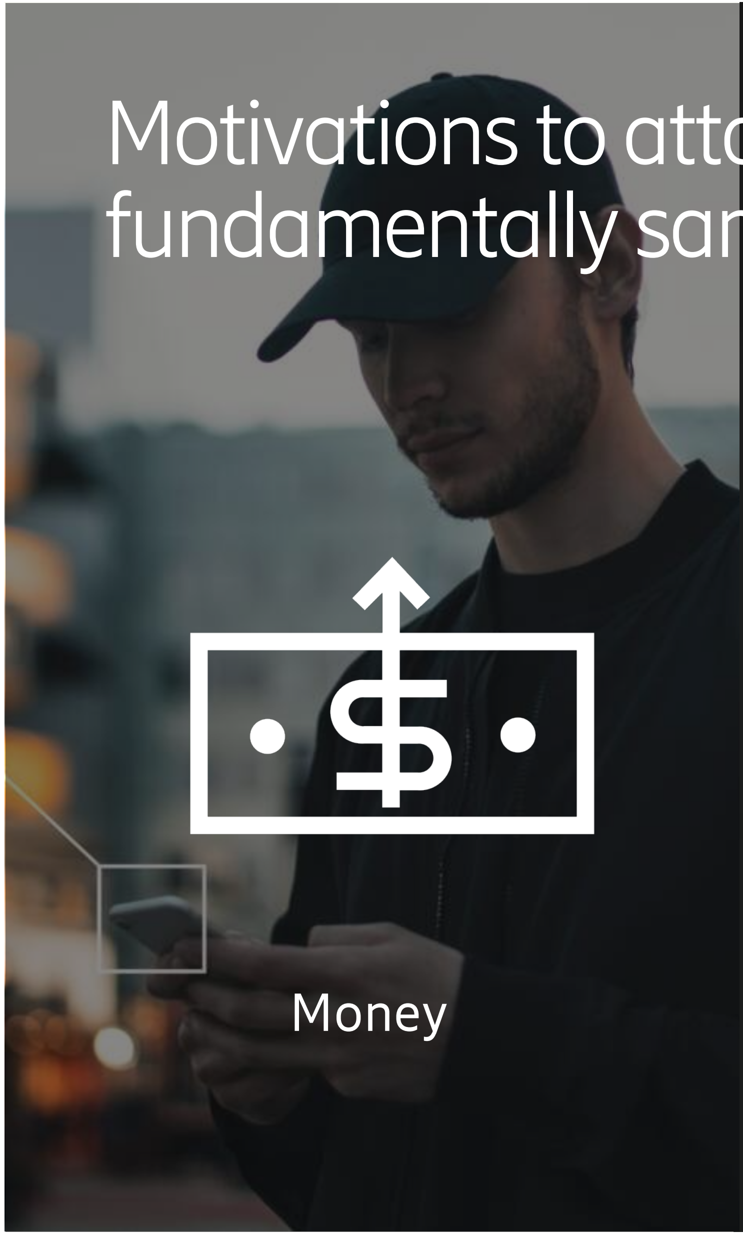
For business:

- Enabler to earn customer trust

For nation-states:

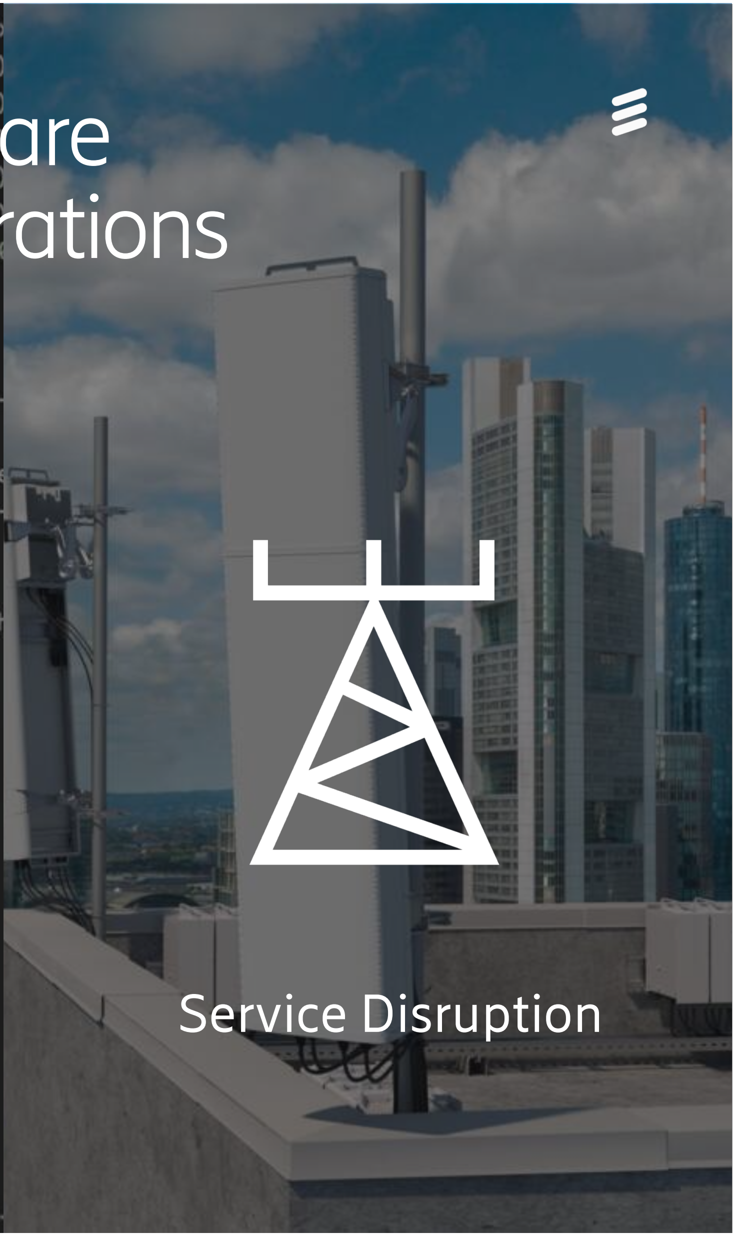
- Investment to national sovereignty

Motivations to attack mobile networks are fundamentally same through the generations



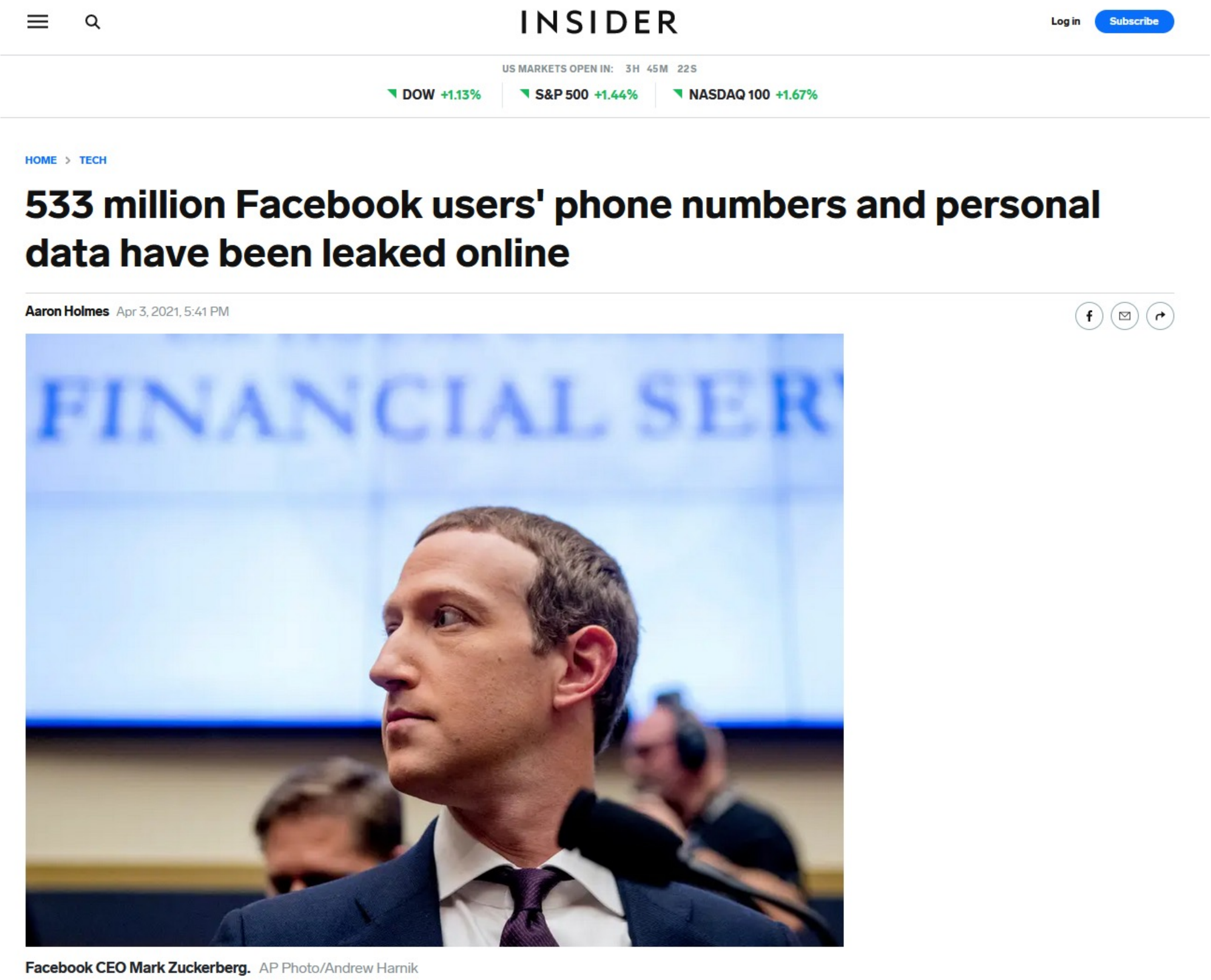
Money

Information



Service Disruption

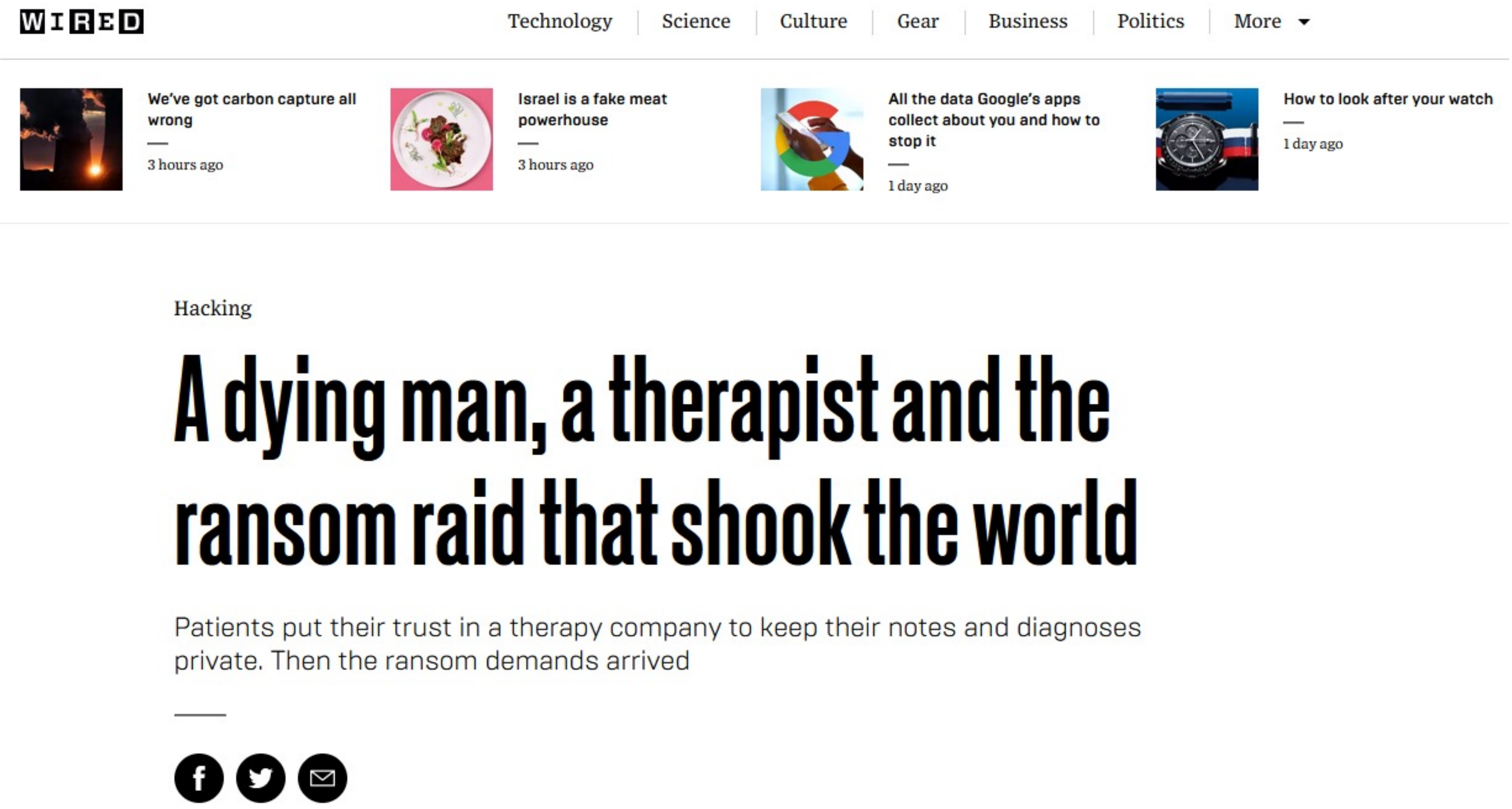
What does security consist of?



533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 5:41 PM

Facebook CEO Mark Zuckerberg. AP Photo/Andrew Harnik



We've got carbon capture all wrong

—

3 hours ago

Israel is a fake meat powerhouse

—

3 hours ago

All the data Google's apps collect about you and how to stop it

—

1 day ago

How to look after your watch

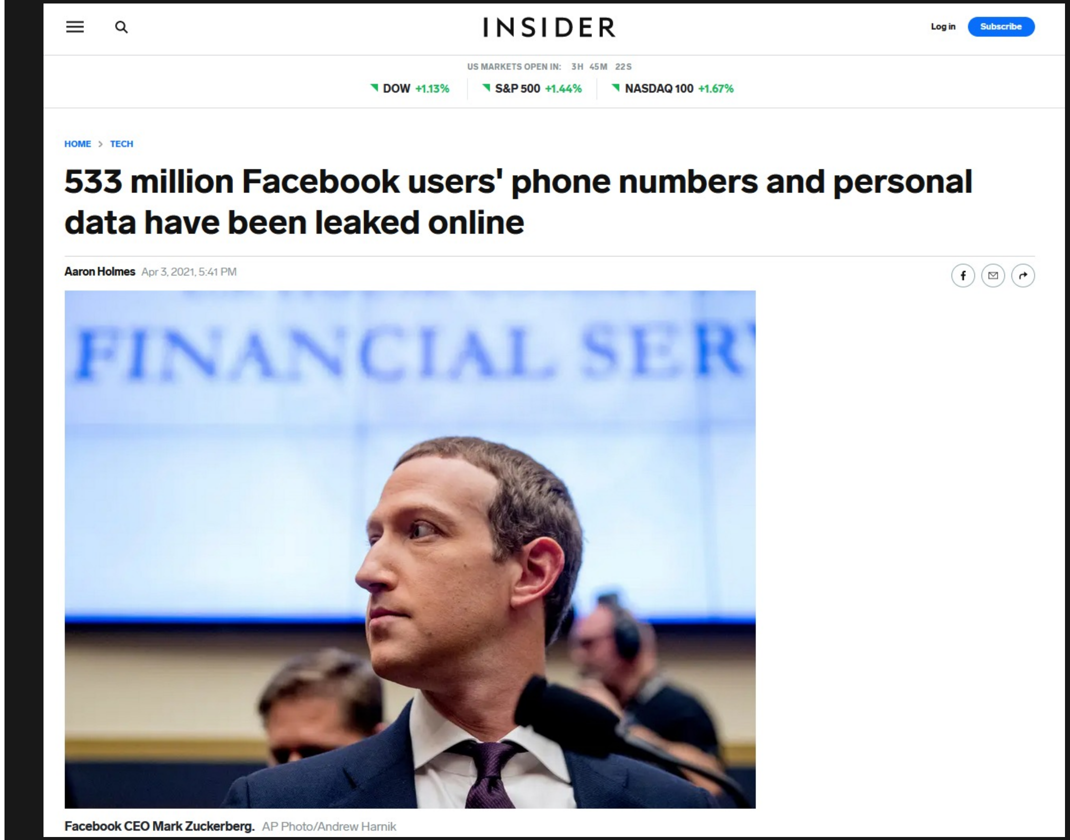
—

1 day ago

Hacking

A dying man, a therapist and the ransom raid that shook the world

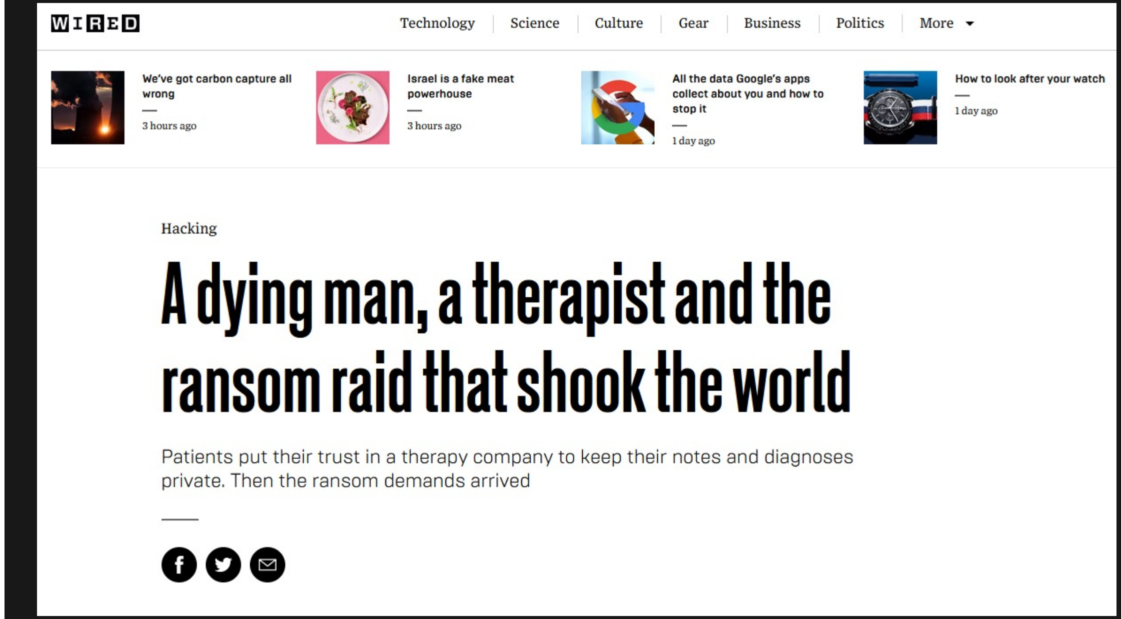
Patients put their trust in a therapy company to keep their notes and diagnoses private. Then the ransom demands arrived



533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 5:41 PM

Facebook CEO Mark Zuckerberg. AP Photo/Andrew Harnik



We've got carbon capture all wrong
—
3 hours ago

Israel is a fake meat powerhouse
—
3 hours ago

All the data Google's apps collect about you and how to stop it
—
1 day ago

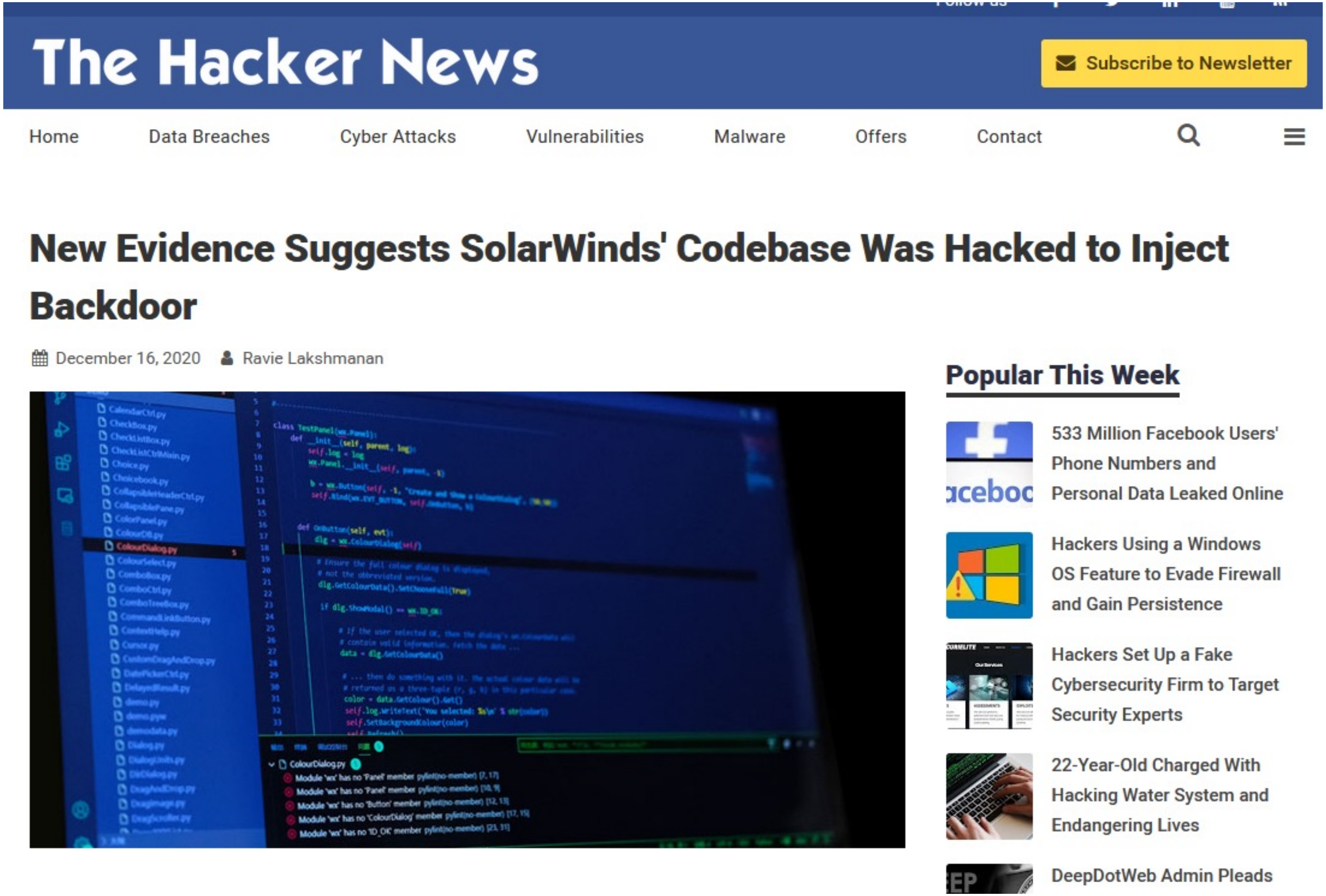
How to look after your watch
—
1 day ago

Hacking

A dying man, a therapist and the ransom raid that shook the world

Patients put their trust in a therapy company to keep their notes and diagnoses private. Then the ransom demands arrived

Confidentiality



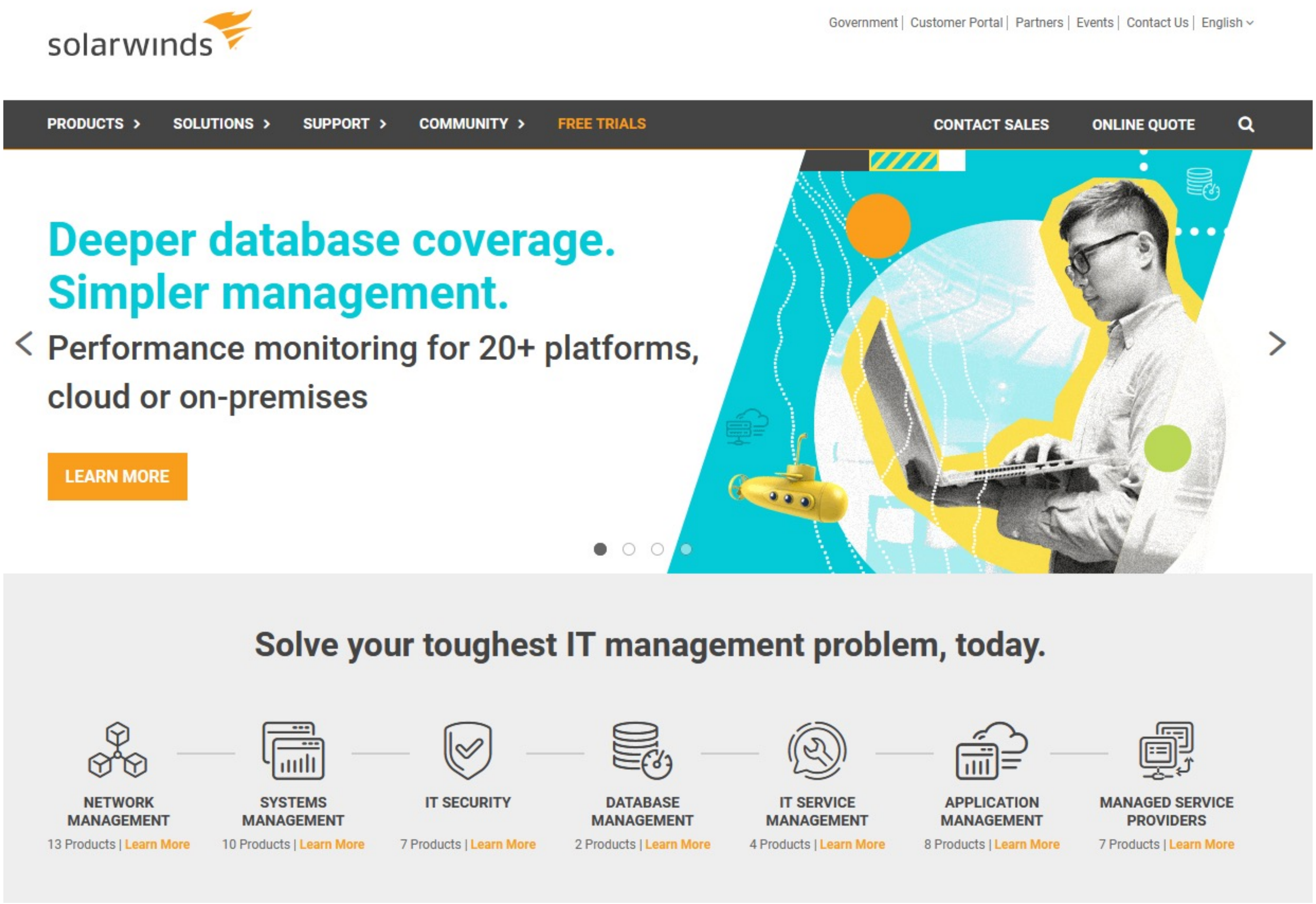
Home Data Breaches Cyber Attacks Vulnerabilities Malware Offers Contact

New Evidence Suggests SolarWinds' Codebase Was Hacked to Inject Backdoor

December 16, 2020 Ravie Lakshmanan

Popular This Week

- 533 Million Facebook Users' Phone Numbers and Personal Data Leaked Online
- Hackers Using a Windows OS Feature to Evade Firewall and Gain Persistence
- Hackers Set Up a Fake Cybersecurity Firm to Target Security Experts
- 22-Year-Old Charged With Hacking Water System and Endangering Lives
- DeepDotWeb Admin Pleads



Deeper database coverage. Simpler management.

Performance monitoring for 20+ platforms, cloud or on-premises

Solve your toughest IT management problem, today.

NETWORK MANAGEMENT	SYSTEMS MANAGEMENT	IT SECURITY	DATABASE MANAGEMENT	IT SERVICE MANAGEMENT	APPLICATION MANAGEMENT	MANAGED SERVICE PROVIDERS
13 Products | Learn More	10 Products | Learn More	7 Products | Learn More	2 Products | Learn More	4 Products | Learn More	8 Products | Learn More	7 Products | Learn More

SolarWinds hackers accessed DHS acting secretary's emails: What you need to know

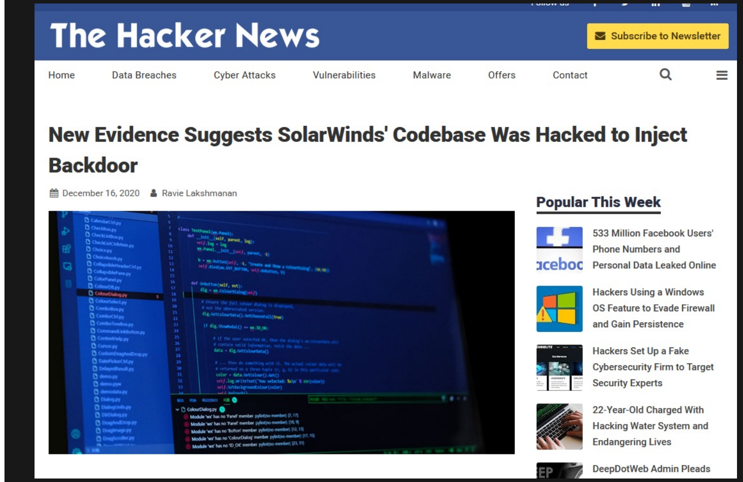
The AP reports that the suspected Russian hacking group breached high-level accounts in DHS, one of nine federal agencies the hackers targeted.

Laura Hautala March 29, 2021 11:45 a.m. PT

▶ LISTEN - 12:11

US intelligence agencies have said Russia is responsible for a major hacking campaign that struck federal agencies and prominent tech companies.

Angela Lang/CNET

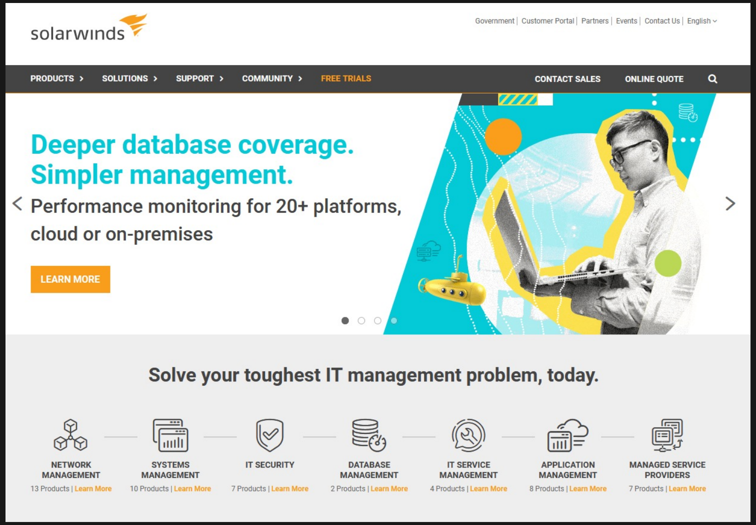


New Evidence Suggests SolarWinds' Codebase Was Hacked to Inject Backdoor

December 16, 2020 Ravie Lakshmanan

Popular This Week

- 533 Million Facebook Users' Phone Numbers and Personal Data Leaked Online
- Hackers Using a Windows OS Feature to Evade Firewall and Gain Persistence
- Hackers Set Up a Fake Cybersecurity Firm to Target Security Experts
- 22-Year-Old Charged With Hacking Water System and Endangering Lives
- DeepDotWeb Admin Pleads

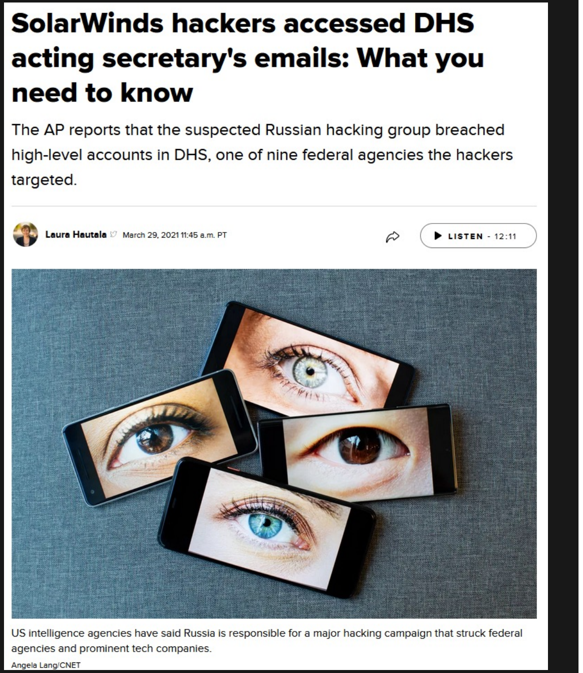


Deeper database coverage. Simpler management.

Performance monitoring for 20+ platforms, cloud or on-premises

Solve your toughest IT management problem, today.

NETWORK MANAGEMENT	SYSTEMS MANAGEMENT	IT SECURITY	DATABASE MANAGEMENT	IT SERVICE MANAGEMENT	APPLICATION MANAGEMENT	MANAGED SERVICE PROVIDERS
13 Products | Learn More	10 Products | Learn More	7 Products | Learn More	2 Products | Learn More	4 Products | Learn More	8 Products | Learn More	7 Products | Learn More



SolarWinds hackers accessed DHS acting secretary's emails: What you need to know

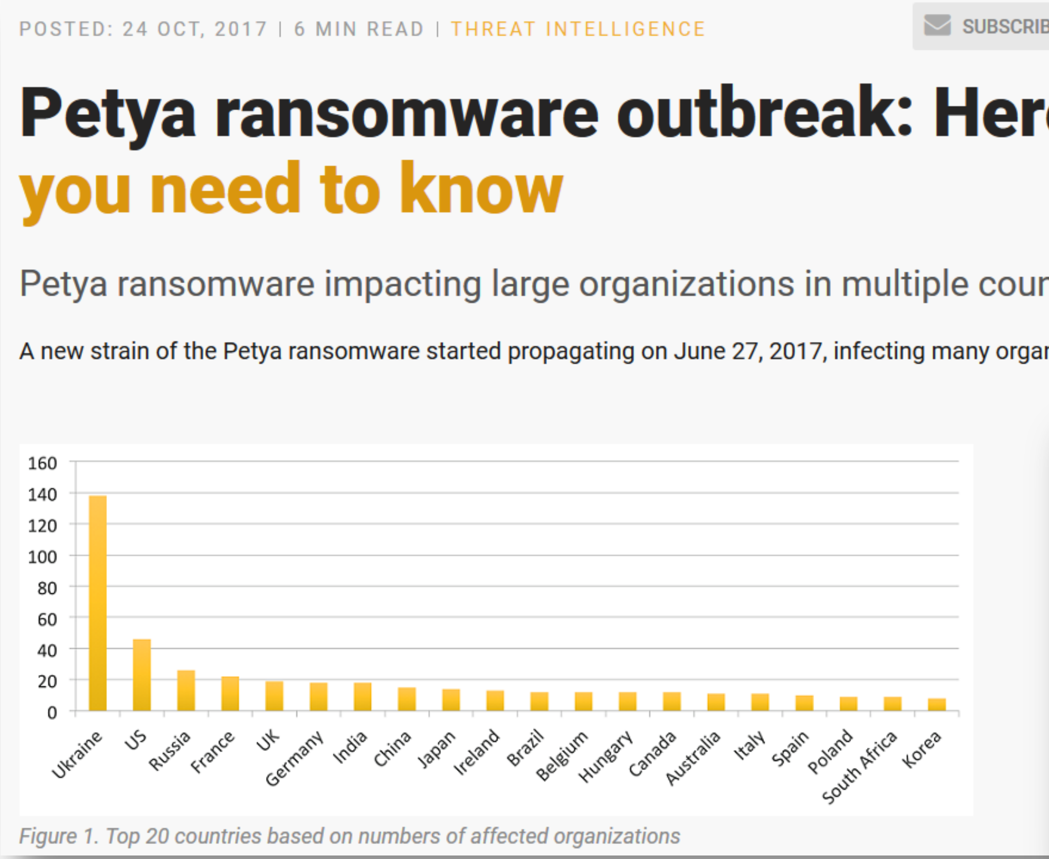
The AP reports that the suspected Russian hacking group breached high-level accounts in DHS, one of nine federal agencies the hackers targeted.

Laura Hautala March 29, 2021 11:45 a.m. PT

US intelligence agencies have said Russia is responsible for a major hacking campaign that struck federal agencies and prominent tech companies.

Angela Lang/CNET

Integrity



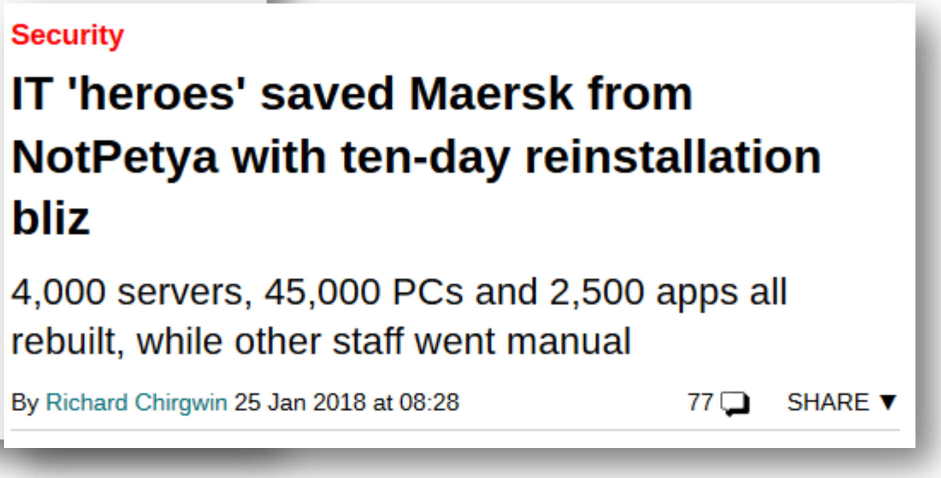
POSTED: 24 OCT, 2017 | 6 MIN READ | THREAT INTELLIGENCE

Petya ransomware outbreak: Here’s what you need to know

Petya ransomware impacting large organizations in multiple countries.

A new strain of the Petya ransomware started propagating on June 27, 2017, infecting many organizations.

Figure 1. Top 20 countries based on numbers of affected organizations

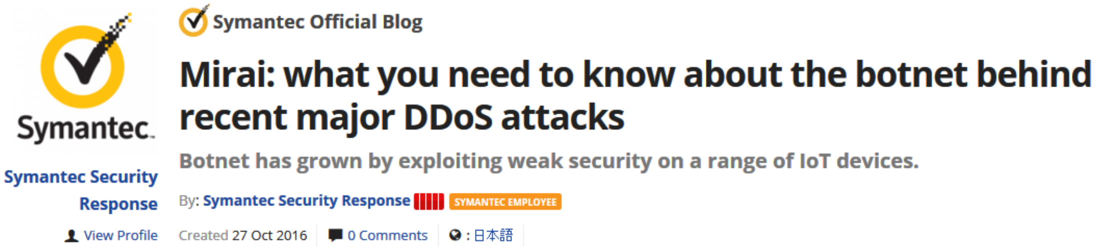


Security

IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz

4,000 servers, 45,000 PCs and 2,500 apps all rebuilt, while other staff went manual

By Richard Chirgwin 25 Jan 2018 at 08:28



Symantec Security Response

View Profile

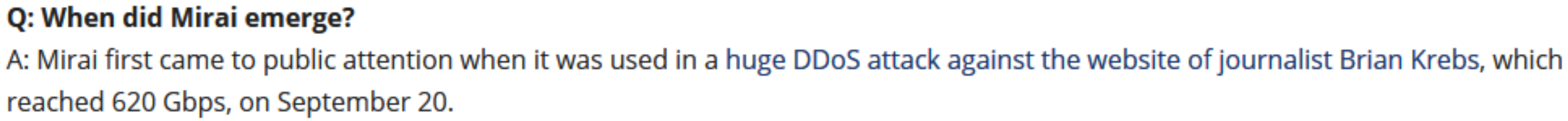
Symantec Official Blog

Mirai: what you need to know about the botnet behind recent major DDoS attacks

Botnet has grown by exploiting weak security on a range of IoT devices.

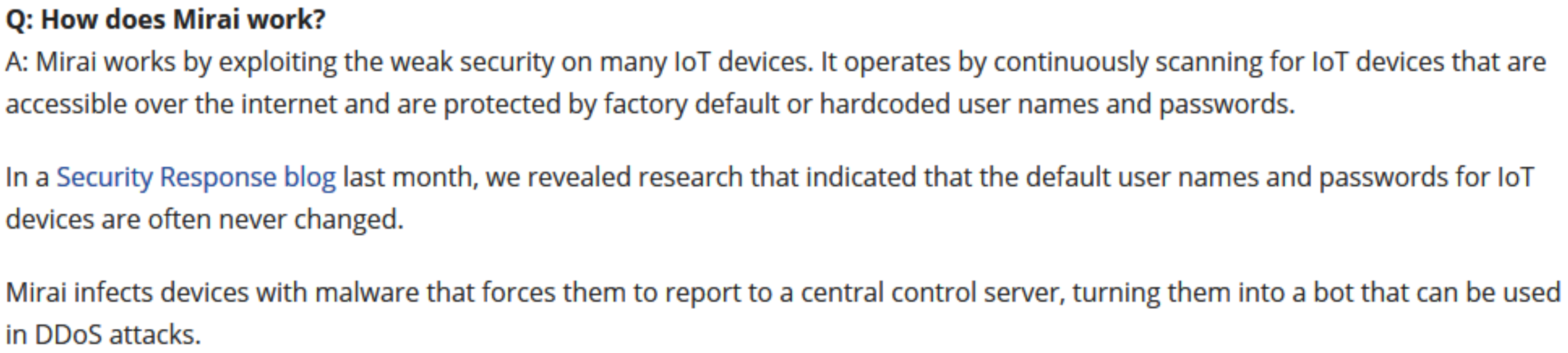
By: Symantec Security Response SYMANTEC EMPLOYEE

Created 27 Oct 2016 | 0 Comments | : 日本語



Q: When did Mirai emerge?

A: Mirai first came to public attention when it was used in a huge DDoS attack against the website of journalist Brian Krebs, which reached 620 Gbps, on September 20.

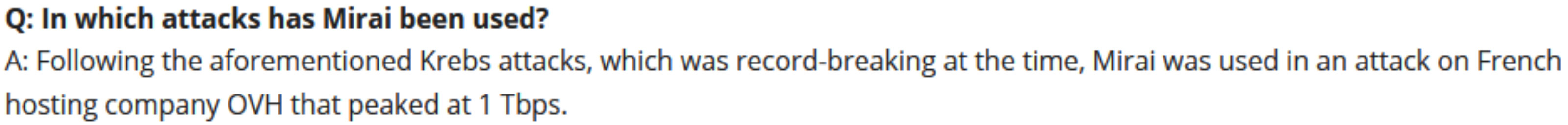


Q: How does Mirai work?

A: Mirai works by exploiting the weak security on many IoT devices. It operates by continuously scanning for IoT devices that are accessible over the internet and are protected by factory default or hardcoded user names and passwords.

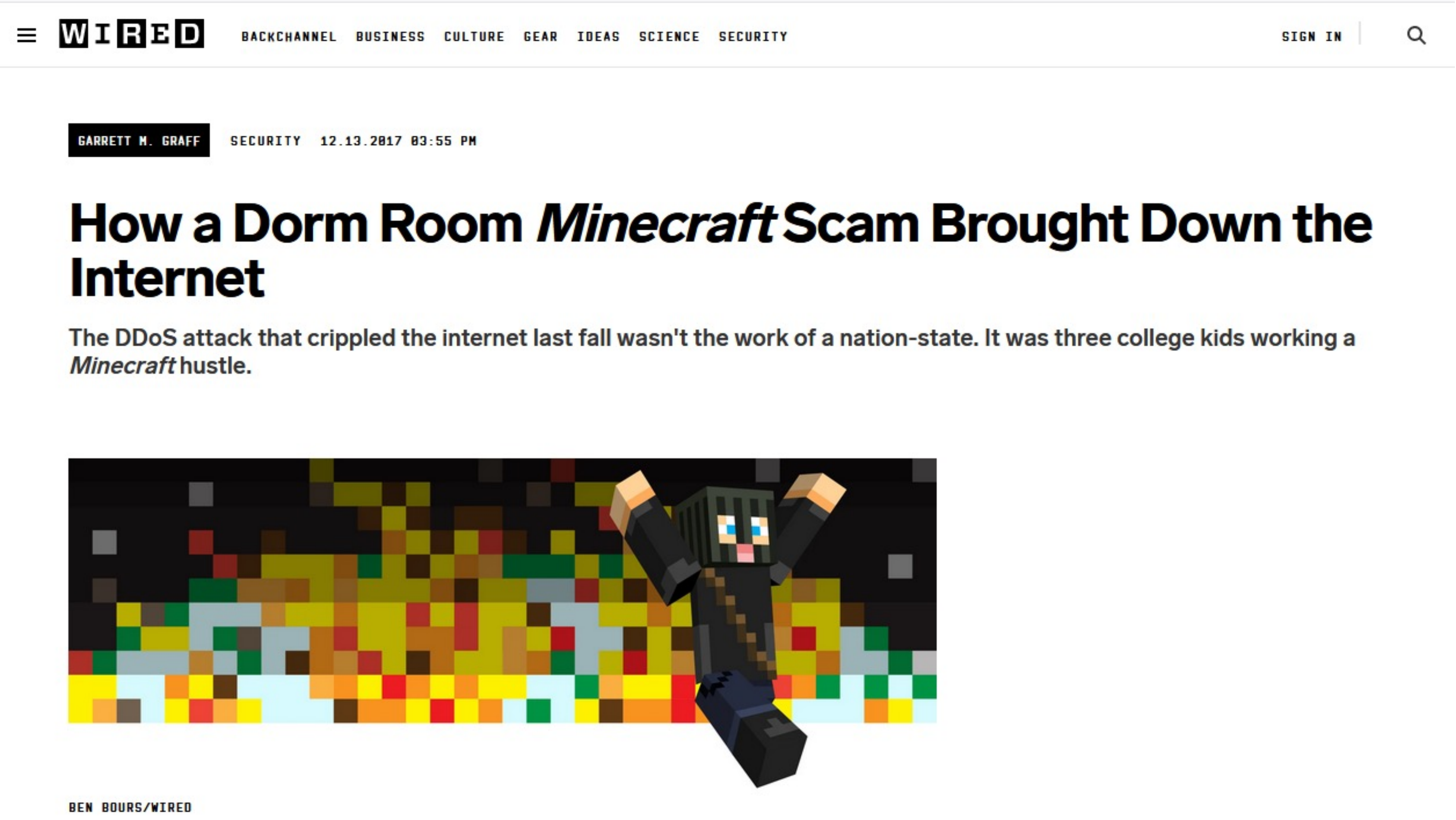
In a Security Response blog last month, we revealed research that indicated that the default user names and passwords for IoT devices are often never changed.

Mirai infects devices with malware that forces them to report to a central control server, turning them into a bot that can be used in DDoS attacks.



Q: In which attacks has Mirai been used?

A: Following the aforementioned Krebs attacks, which was record-breaking at the time, Mirai was used in an attack on French hosting company OVH that peaked at 1 Tbps.



GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

The DDoS attack that crippled the internet last fall wasn't the work of a nation-state. It was three college kids working a *Minecraft* hustle.

BEN BOURS/WIRED

Security news that informs and inspires

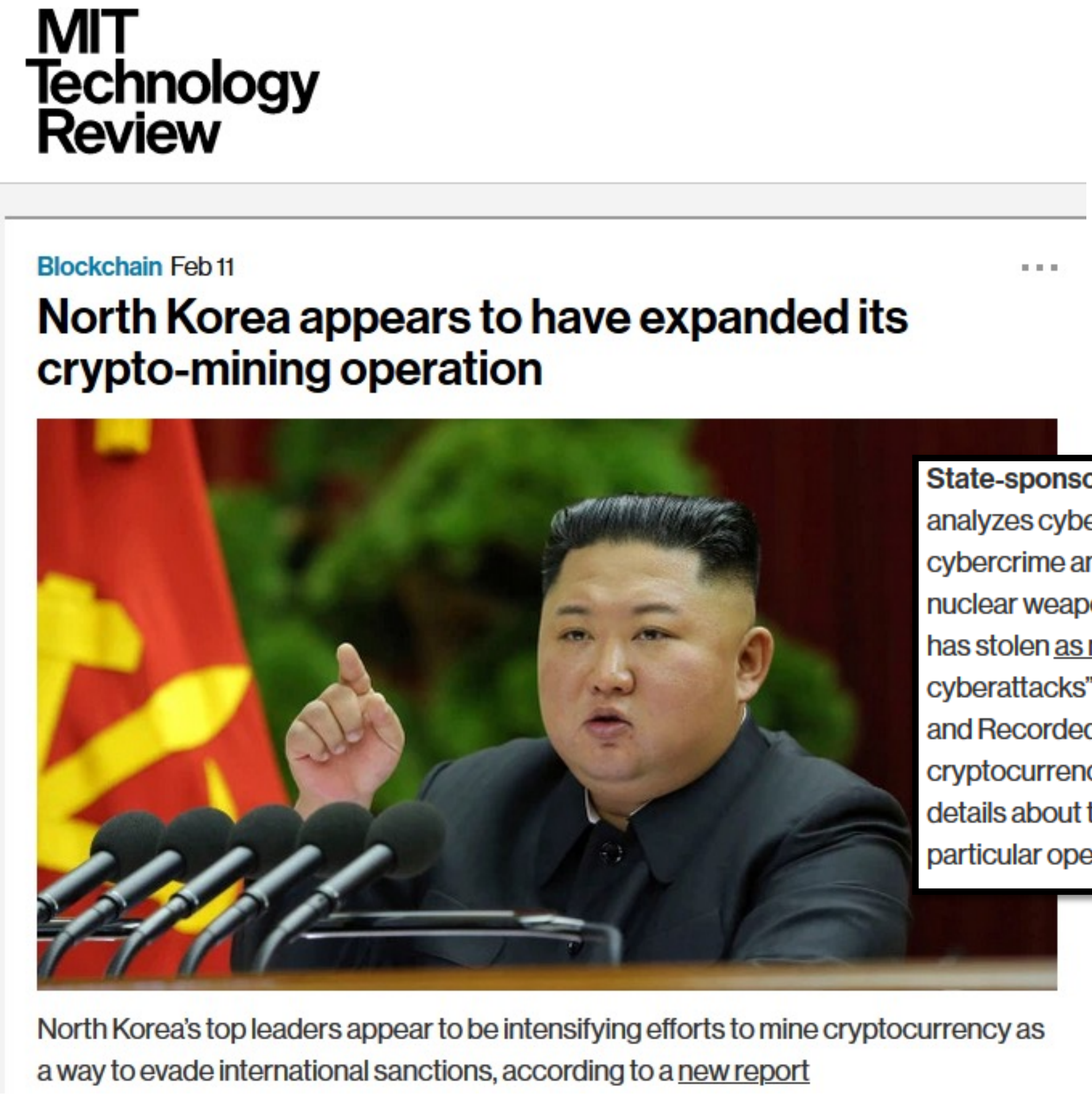
May 4, 2020

SALTSTACK FLAW USED IN NUMEROUS ATTACKS

By Dennis Fisher

The attacks that hit Ghost and Xen Orchestra were relatively simplistic and appear to have only installed cryptocoin mining scripts on the exploited machines. The exploitation attempts look to be coming from a coin mining botnet and there are several exploits for the code execution flaw available already. In its account of the attack, Ghost described a scenario that was quite similar to the one at Xen Orchestra.

“Our investigation indicates that a critical vulnerability in our server management infrastructure (Saltstack, CVE-2020-11651 CVE-2020-11652) was used in an attempt to mine cryptocurrency on our servers. The mining attempt spiked CPUs and quickly overloaded most of our systems, which alerted us to the issue immediately,” the Ghost timeline says.



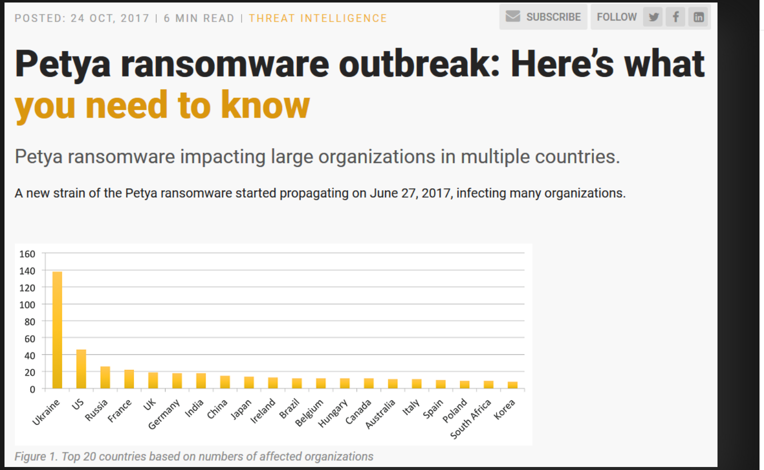
MIT Technology Review

Blockchain Feb 11

North Korea appears to have expanded its crypto-mining operation

North Korea's top leaders appear to be intensifying efforts to mine cryptocurrency as a way to evade international sanctions, according to a new report

State-sponsored crypto-crime: The report by Recorded Future, a US company that analyzes cybersecurity threats, details the efforts of Kim Jong-un's regime to use cybercrime and cryptocurrency to get around sanctions meant to curb the nation's nuclear weapons program. The United Nations recently estimated that North Korea has stolen as much as $2 billion using "widespread and increasingly sophisticated cyberattacks" on financial institutions and cryptocurrency exchanges. Both the UN and Recorded Future had reported previously that in addition to stealing cryptocurrency, the regime had also started mining it. The new report adds more details about the mining effort and suggests that North Korea is expanding this particular operation.



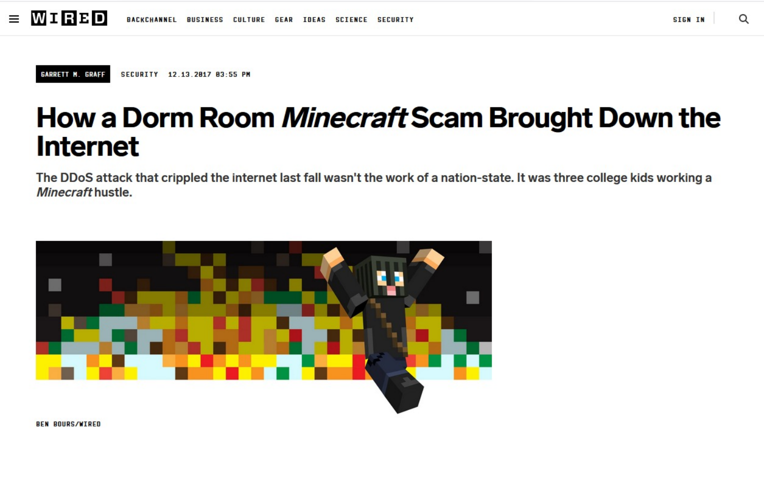
POSTED: 24 OCT, 2017 | 6 MIN READ | THREAT INTELLIGENCE

Petya ransomware outbreak: Here's what you need to know

Petya ransomware impacting large organizations in multiple countries.

A new strain of the Petya ransomware started propagating on June 27, 2017, infecting many organizations.

Figure 1. Top 20 countries based on numbers of affected organizations

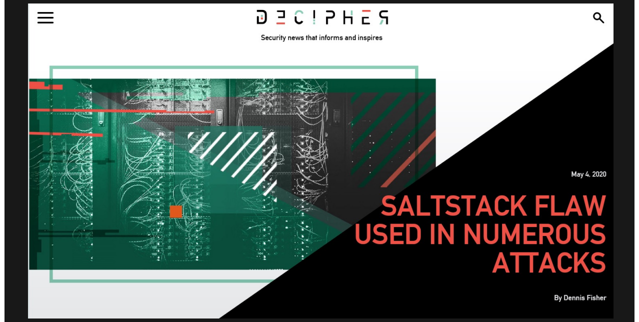


GARRETT M. GRAFF SECURITY 12.13.2017 03:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

The DDoS attack that crippled the internet last fall wasn't the work of a nation-state. It was three college kids working a *Minecraft* hustle.

BEN BOURS/WIRED



Security news that informs and inspires

May 4, 2020

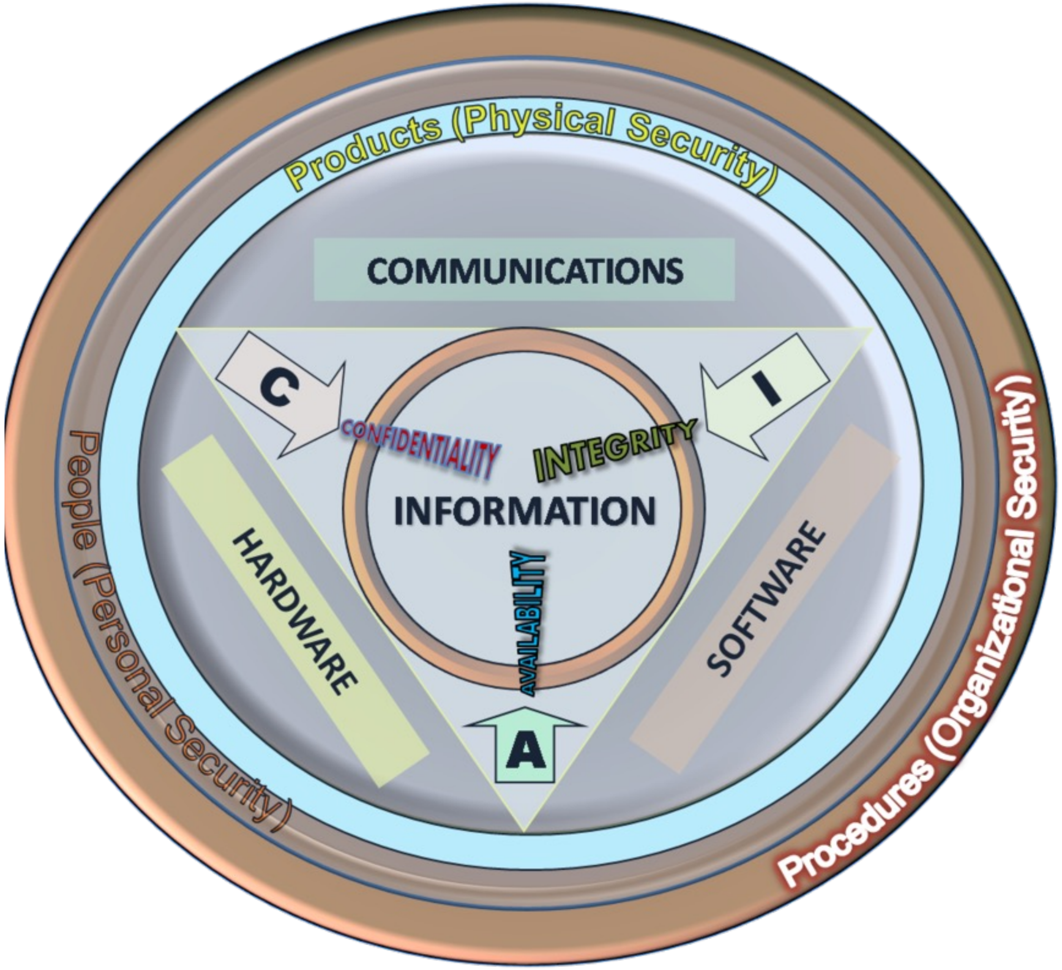
SALTSTACK FLAW USED IN NUMEROUS ATTACKS

By Dennis Fisher

Availability

One definition of (Information) Security

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.“ —Committee of National Security Systems, 2010


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

— Source: Wikipedia

Privacy

गोपनीयता

Riservatezza

Intimitate

μυστικότητα

нууцлал

Magánélet

Privacidad

Yksityisyyden suoja

निजता

Confidentialité

Integritet

Mahremiyet

隐私

конфиденциальность

Security
Sicurezza
Securité
Securidad
Säkerhet
Sicherheit
Securitate
Sigurnosti
Tietoturva
Безопасность

Dario Casella

Head of Ericsson Product Privacy Office

What is privacy and data protection?

- Respecting fundamental rights to **protect personal data** and privacy*
- **Personal data:**
  - Any information which are related to an identified or identifiable natural person
- **Processing personal data:**
  - Any operation performed on personal data such as: collection, recording, storage, adaptation, use, disclosure by transmission, dissemination, erasure, etc.

** Article 7 and 8 of the Charter of Fundamental Rights of the European Union*

Personal data examples

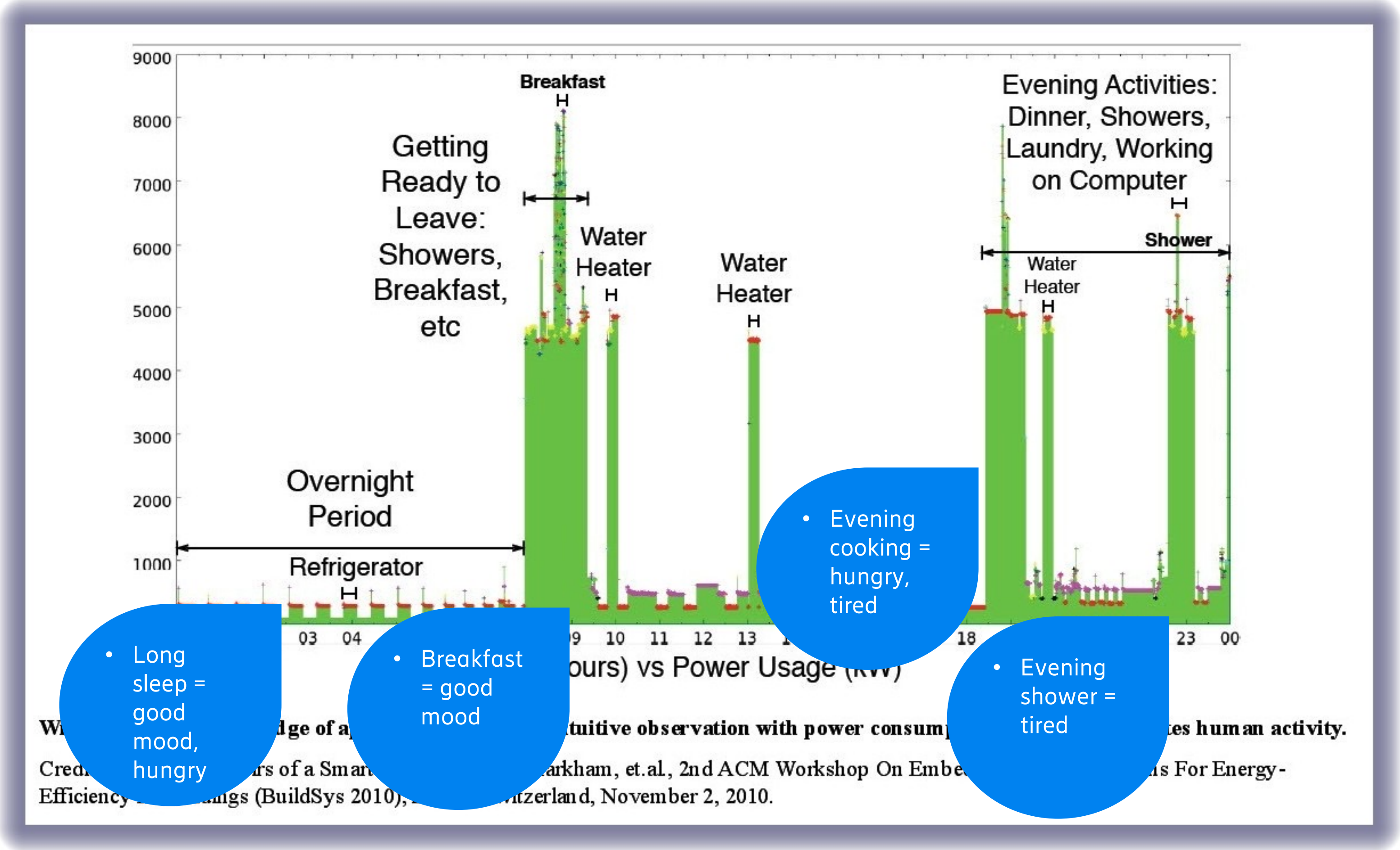
- First Name
- Last Name
- Phone number
- E-mail
- Home address
- IMEI, IMSI, MSISDN
- IP address, location
- MAC address
- Session history
- Call history
- Subscribed services
- Purchase history
- Credit card data
- Medical records
- Health records
- Biometric data
- Financial records
- Criminal records
- Social Security number
- Religious beliefs
- Sexual orientation
- Trade union memberships
- Behavioral data
- Identifiers
- Cookies
- Trackers
- Profiles

So, privacy is about protecting personal data.

What does it actually mean, in practice?
And is it so simple and straight forward?

Internet of things – electricity data

How Smart Meters Invade Individual Privacy



Wi dge of a tuitive observation with power consum tes human activity.

Cred rs of a Smar arkham, et.al., 2nd ACM Workshop On Embe s For Energy-Efficiency ngs (BuildSys 2010), tzerland, November 2, 2010.

- Long sleep = good mood, hungry

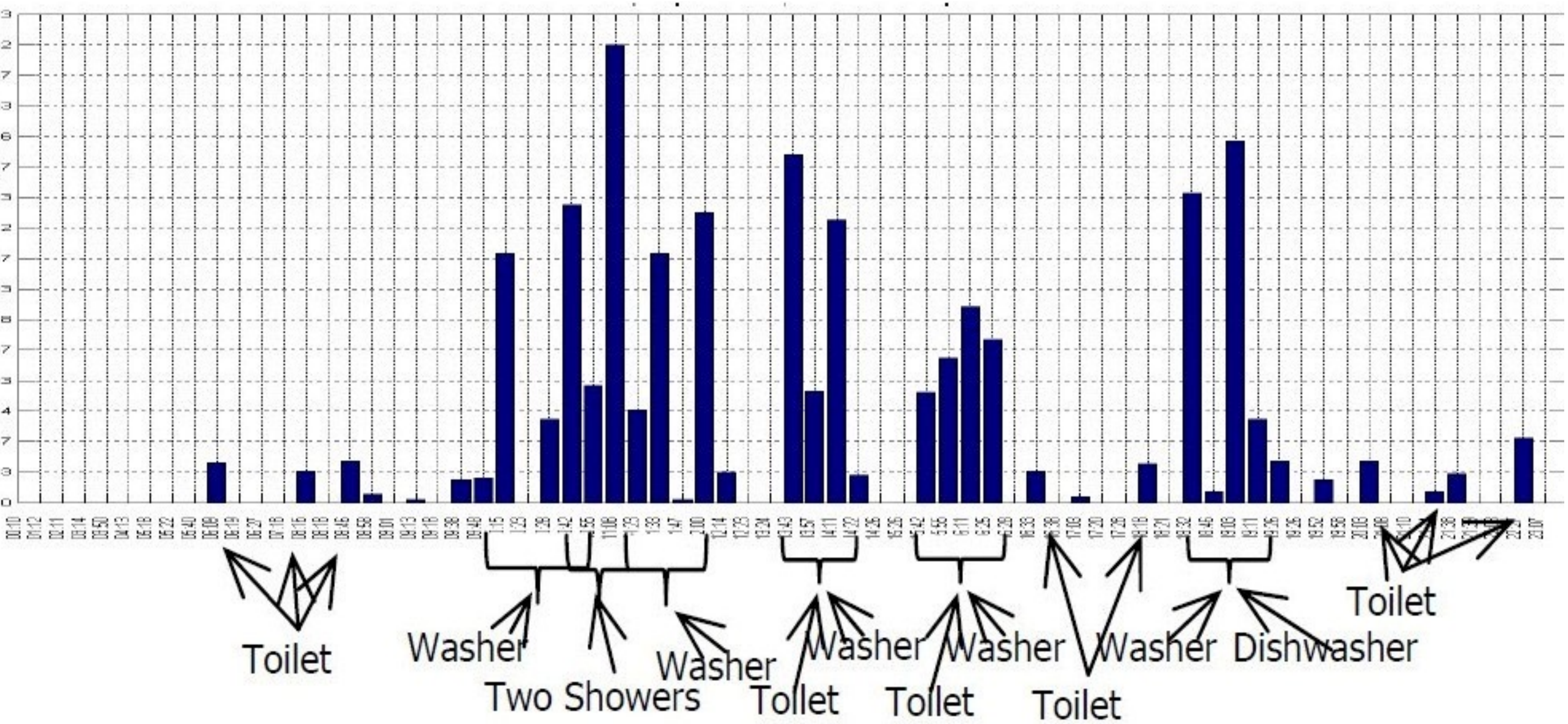
- Breakfast = good mood

- Evening cooking = hungry, tired

- Evening shower = tired

Internet of things – water data

How Smart Meters Invade Individual Privacy



Artificial Intelligence and privacy

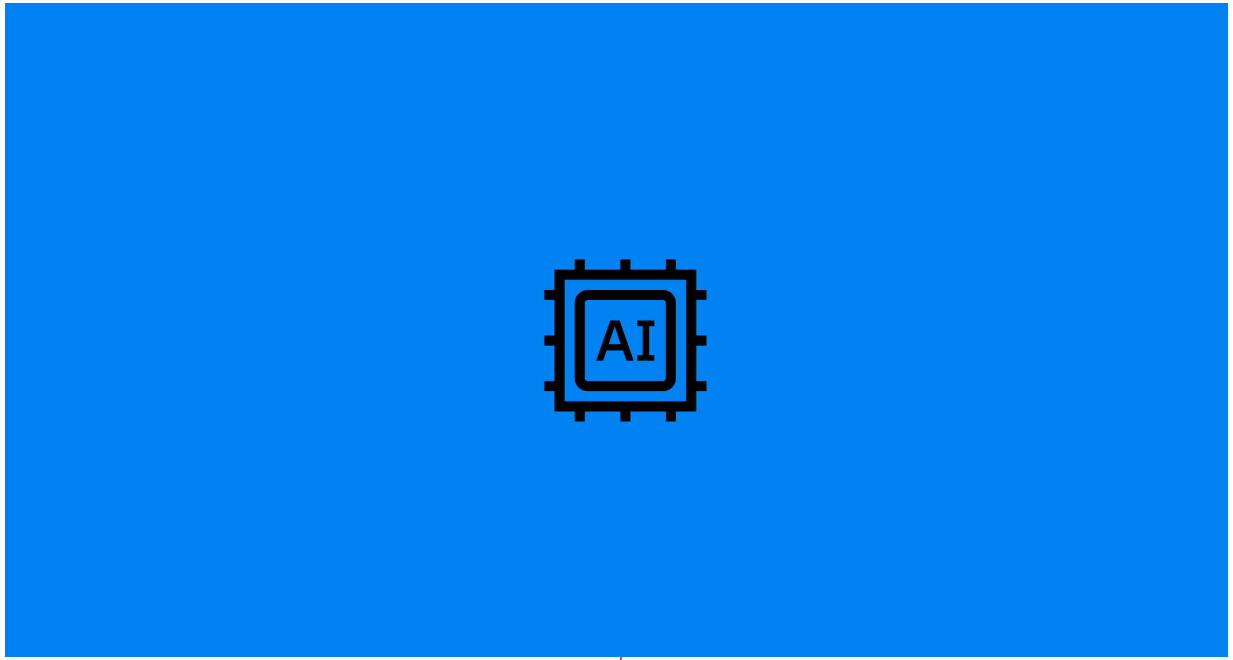
Artificial intelligence and privacy

Report, January 2018

Datatilsynet

The Norwegian Data Protection Authority

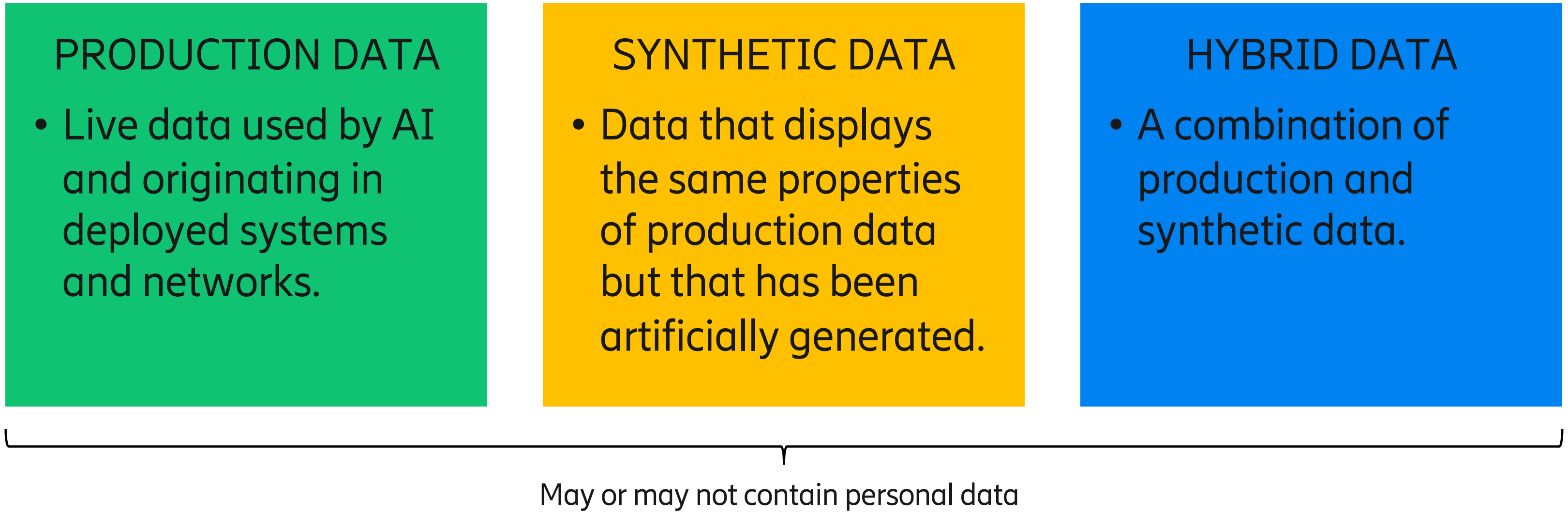
- A decision tree is one of the simplest models
- Start at the top and selects a branch on the lower level
- Such a simple model offers great transparency
- With increasing amount of data, it becomes difficult for a person to obtain an overview and understanding



Example of BIAS: an inflection point when the model “decides” that a hungry person is not productive

BIAS can be unfair and can have high impact privacy, human rights, diversity, etc..

Protecting privacy by using different types of data sets in AI



PRODUCTION DATA

- Live data used by AI and originating in deployed systems and networks.

SYNTHETIC DATA

- Data that displays the same properties of production data but that has been artificially generated.

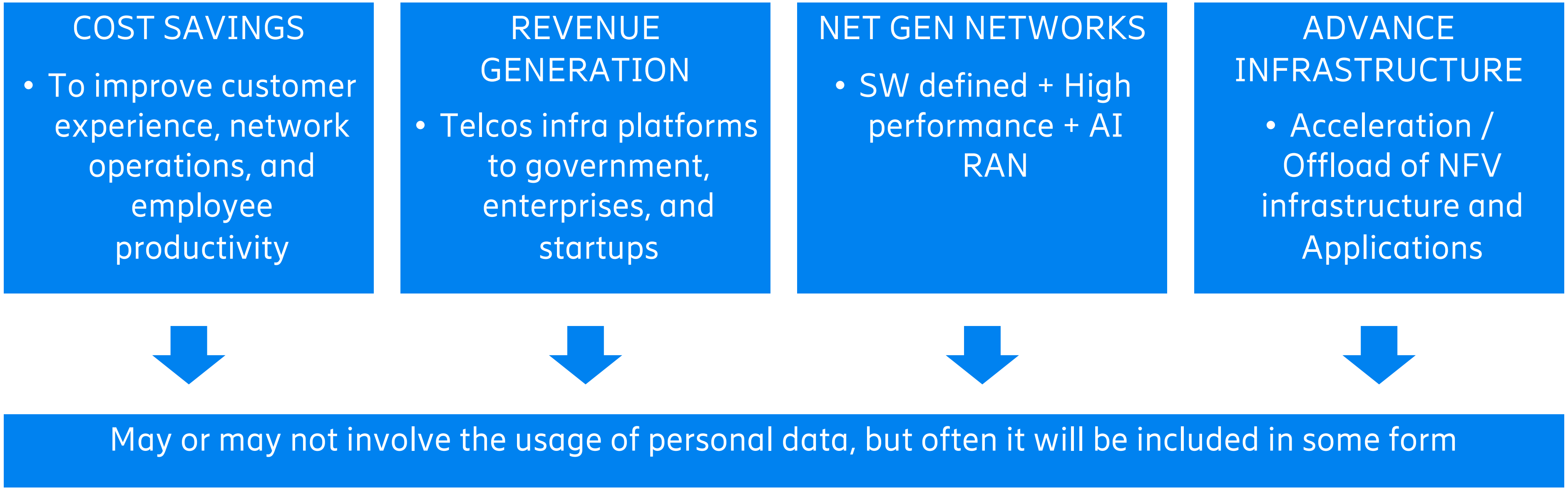
HYBRID DATA

- A combination of production and synthetic data.

May or may not contain personal data

- Each data set may be naturally skewed/asymetric, that is NOT considered as bias. i.e. more data about men than women in a data set
- **AI results can be unfair or "biased"**. This bias has to be considered when assessing privacy impact.

Examples of use cases in telecom with potential impact on security and privacy (with or without AI)



COST SAVINGS

- To improve customer experience, network operations, and employee productivity

REVENUE GENERATION

- Telcos infra platforms to government, enterprises, and startups

NET GEN NETWORKS

- SW defined + High performance + AI RAN

ADVANCE INFRASTRUCTURE

- Acceleration / Offload of NFV infrastructure and Applications

May or may not involve the usage of personal data, but often it will be included in some form

General Data Protection Regulation (GDPR)

- Enacted: 25th May 2018
- Considered to be the "gold standard" for privacy regulations
- Applicable across all 27 EU Member States, and select other partner nations
- Has formed the basis for other regulations around the globe
- Designed to be "future proof" by the European Union

The protection of natural persons in relation to the processing of personal data is a fundamental right…everyone has the right to the protection of personal data concerning him or her.

GDPR Recitals 1

Some of the relevant privacy regulations in the world

- The **General Data Protection Regulation (GDPR)** was arguably the first comprehensive data protection regulation.
- The GDPR is applicable in the EU and EEA, and many other jurisdictions use it as a blueprint for their regulations.

- The **Digital Personal Data Protection Bill (DPDPB)** is India's 4th attempt at a data protection regulation since 2017.
- The DPDPB imposes stricter requirements on data controllers that process large volumes of personal data.

- The **California Privacy Rights Act (CPRA)** applies only to California and is the US's most comprehensive privacy law
- CPRA is also used as a blueprint for other U.S. states to issue their own laws.

- **Personal Information Protection Law (PIPL)** established a comprehensive regulatory framework for personal data protection in China.
- PIPL also imposes stricter requirements on data controllers that process large volumes of personal data.

- Australia has a mix of federal, state, and territory laws that regulate the protection of personal data.
- The federal **Privacy Act 1988** that applies to private sectors, and state level regulations apply to government agencies.

- Japan's **Act on the Protection of Personal Information (APPI)** was adopted already in 2003. Since then, it has been amended two times, aligning the Act more with the GDPR.
- The APPI will be updated every three years if necessary to ensure that it keeps up with the latest technical developments.

- The **Personal Data Protection Law (PDPL)** is Saudi Arabia's first standalone data protection law. Saudi Arabia's supervisory authority has the mandate to release supplementary laws.

- The **Protection of Personal Information Act (POPIA)** was passed already in 2013, but came into force in 2020.
- The Act regulates the protection of personal data processed by both public and private bodies.

Many jurisdictions use GDPR as the blueprint for their data protection regulations

What can go wrong - Privacy harms & telecom data

Basic privacy violation

- Death or bodily harm
- Loss of personal freedom of movement
- Loss of freedom of speech, political opinion, religious beliefs

Financial violation

- Financial damage to personal assets
- Personal monetary loss or fraud
- Blocked or differential access to credit or services
- Negative impact on employment

Non-compliance violation

- Violation of privacy law, customer contract or market access GPRs
- Loss of control over the purposes of processing of personal data
- Inability to exercise privacy rights

Reputation violation

- Severe damage to personal reputation, family name reputation
- Subject to public embarrassment
- Bias, stereotyping, unlawful discrimination

Increased enforcement, increased fines

Biggest fines outside EU – China fines Didi for ~€1.1bn

Didi collected a vast number of screenshots, user clipboard information, and passenger face recognition information for users' phones. The drivers' driver IDs were also stored in plain text.

Protection of children's personal data taken very seriously

Meta fined €405m, Epic Games settled for USD520m, and TikTok fined £27m for violating children's personal data

Using AI to improve your services? Think again

A Hungarian bank was fined €670k for the unlawful use of AI. The AI was used to analyze the emotional state of the customers to determine whether they should be called back.

Meta can't catch a break

On top of the €405m fine, Meta was further fined €265M for an incident in 2021 that leaked the data of 533 million Facebook users.

EU data protection regulators issued a record total of **€2.92 billion** in fines last year. This is a 168% increase from the previous year.

Privacy by Design and Default

Regulatory Obligations

Laws such as the GDPR require it to be in place

Customer Requirements

Collected from various sources. Can put more demanding rules on us

Company Policy and Strategy

Own ambition level and strategy; Group Directive: GPRs

Best Practices and Lessons Learned

What we have learned and experienced, using our expertise

Threat modelling

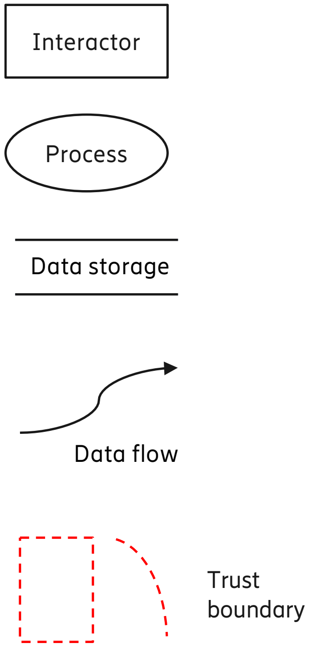
- Basic concepts
- Drawing a data flow diagram
- Threat models
- Real life example

Threat? Risk? Vulnerability?

- Threat: the possibility that an **adverse event** would happen
- Risk: the probability than an **adverse event** materializes, causing an impact
- Vulnerability: a weakness that can be exploited to generate the **adverse event**

The Data Flow Diagram notation

Notation



Interactor

Process

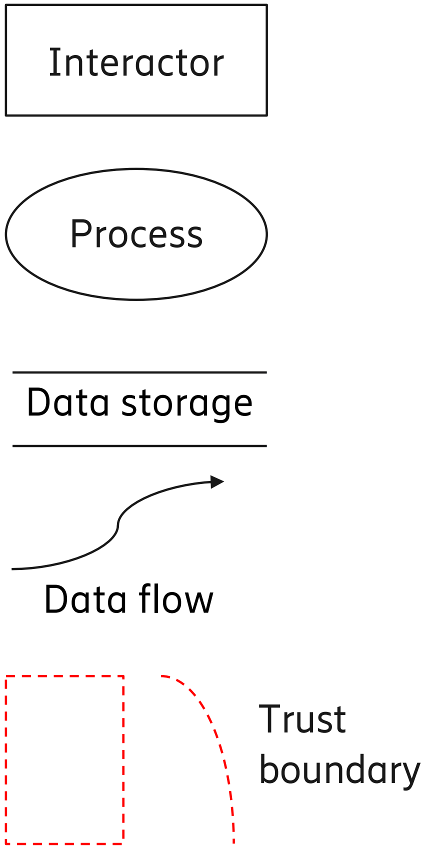
Data storage

Data flow

Trust boundary

Build understanding (example)

Data Flow Diagram (DFD)



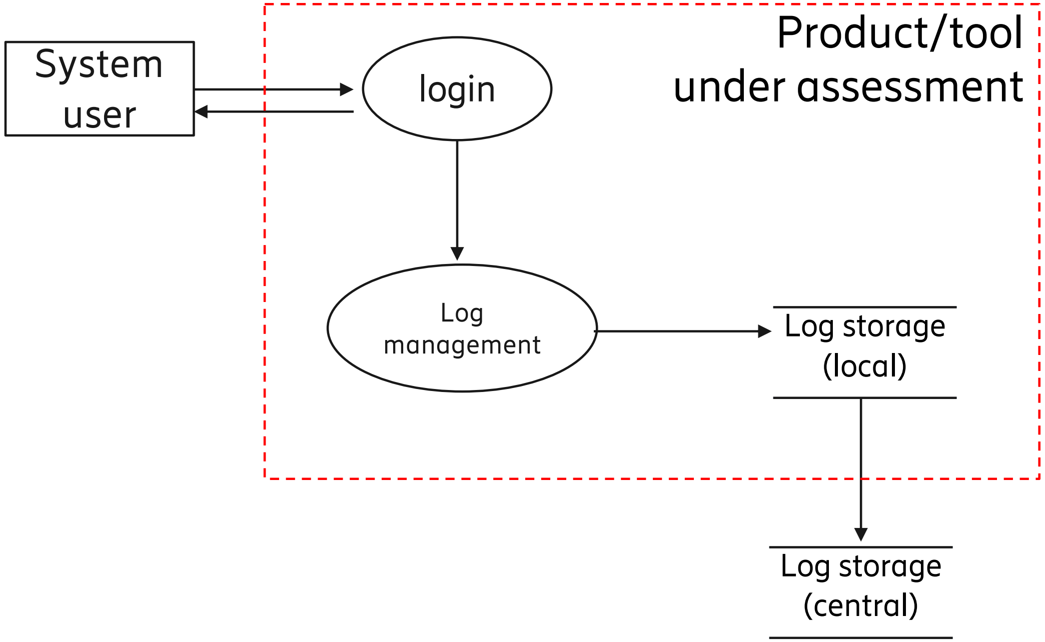
Interactor

Process

Data storage

Data flow

Trust boundary



System user

login

Log management

Log storage (local)

Log storage (central)

Product/tool under assessment

STRIDE, TRIM, LINDDUN

STRIDE	
Spoofing	Authentication (Authenticity)
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

TRIM	
Transfer	Provenance, Chain of custody
Retention Removal	Proportionality Purpose limitation
Inference	Pseudonymity Anonymity, Detectability, Identifiability
~~Minimization~~ Maximization	Minimization

LINDDUN	
Linkability	Unlinkability
Identifiability	Unidentifiability
Non-repudiation	Repudiation
Detectability	Undetectability
Disclosure of Information	Confidentiality
Unawareness	Awareness
Non-compliance	Compliance

First column = threats

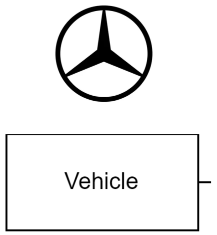
Second column = properties to safeguard

Example scenario: Gateless Parking System

Imaginary training example

- Shopping mall has installed gateless parking system on their garage
- Video camera with automatic license-plate recognition
- Vehicle owner data retrieved from national database
- Payment by app
- Invoices sent to vehicle owners who exit without paying

Example scenario: Data flow diagram



Vehicle

Example security threats

Spoofing

- Customer fakes license plate number to avoid parking fees

Tampering

- License plate number containing SQL injection could harm the integrity of the database

Repudiation

- Customer denies having visited parking garage
- What if car with same LPN enters twice, or if car doesn't leave at all

Information disclosure

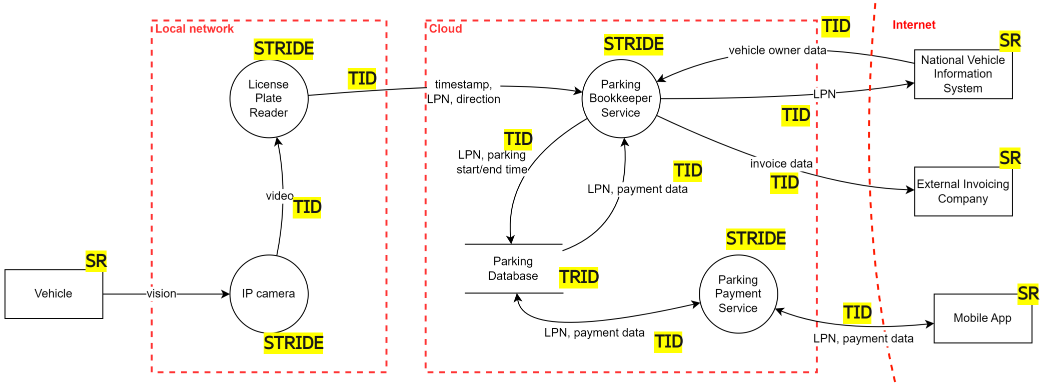
- Parking information containing personal data is stolen from unencrypted database

Denial of Service

- Too many packets sent to Parking Bookkeeper Service could make system unresponsive

Elevation of Privilege

- Malformed packets sent to Parking Bookkeeper Service could let attacker exploit vulnerability and gain control of service



	S	T	R	I	D	E
Interactor	X		X			
Data flow		X		X	X	
Data store		X	?	X	X	
Process	X	X	X	X	X	X

Example privacy threats using TRIM

Personal data in this case

- LPN, vehicle owner info, payment info, times entered/exited garage

Transfer

- Legislatorial and contractual obligations are not followed when transferring personal data to public cloud and to external companies

Retention/Removal

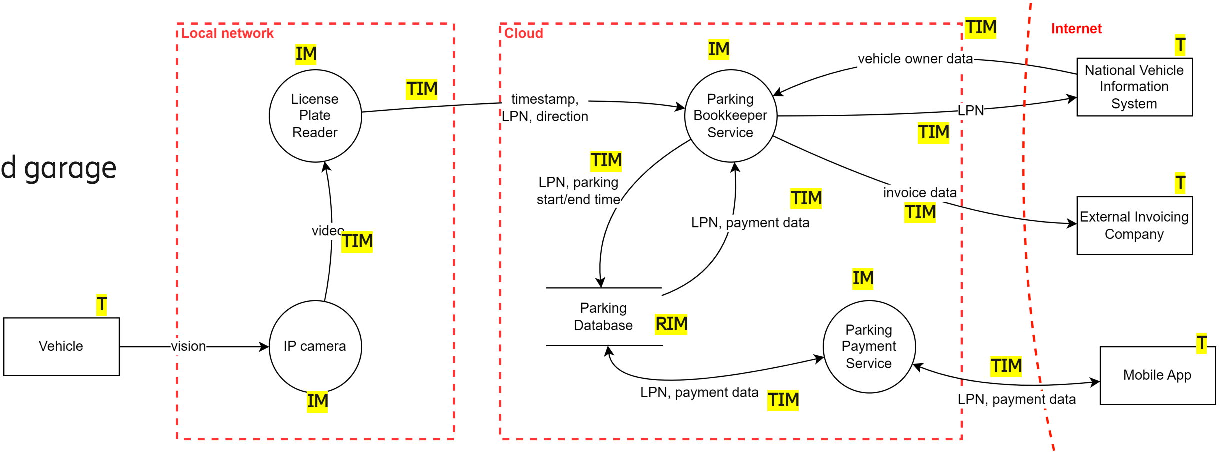
- Retention times are not specified and followed for personal data in database

Inference

- LPN + parking time data could be used to deduce shopping behavior and interests for targeted campaigns

Minimization

- National Vehicle Information System returns excessive vehicle owner info which are retained in Parking Database



	T	R	I	M
Interactor	X			
Data flow	X		X	X
Data store		X	X	X
Process			X	X

What else could go wrong?

Let’s discuss!

What else?

Personal data in this case

- LPN, vehicle owner info, payment info, dates and times entered/exited garage, biometric data captured by license plate reader, Make, model and condition of vehicle, presence of passengers.

Transfer

- Legislatorial and contractual obligations are not followed when transferring personal data to public cloud and to external companies. Use of sub-processors without knowledge and authorization by data controller, e.g., IT support provided from 3rd country, cloud provider using personal data for own purposes and without legal basis.

Retention/Removal

- Retention times are not specified and followed for personal data in database. Removal instruction is not propagated to sub-processors or cannot be audited. Data is insufficiently redacted or de-identified. No DSAR policy, no mechanisms to respond to DSAR. Data cleared but not permanently deleted. Trivial de-identification applied.

Inference

- LPN + parking time data could be used to deduce shopping behavior and interests for targeted campaigns. Presence or absence of passengers can reveal civic status or family composition (e.g., small children). Visiting patterns may reveal associations with other individuals (VIPs, affairs, journalists, diplomats, doctors, police). Multiple parking patterns may reveal place of employment, place of worship, hobbies, schools… Car condition or model may reveal purchase power or ideology. Presence of quasi-identifiers or public information make it trivial to re-identify. Query response reveals presence of item of interest, even without revealing identity (yet), e.g., unlimited queries, too helpful error messages.

Minimization

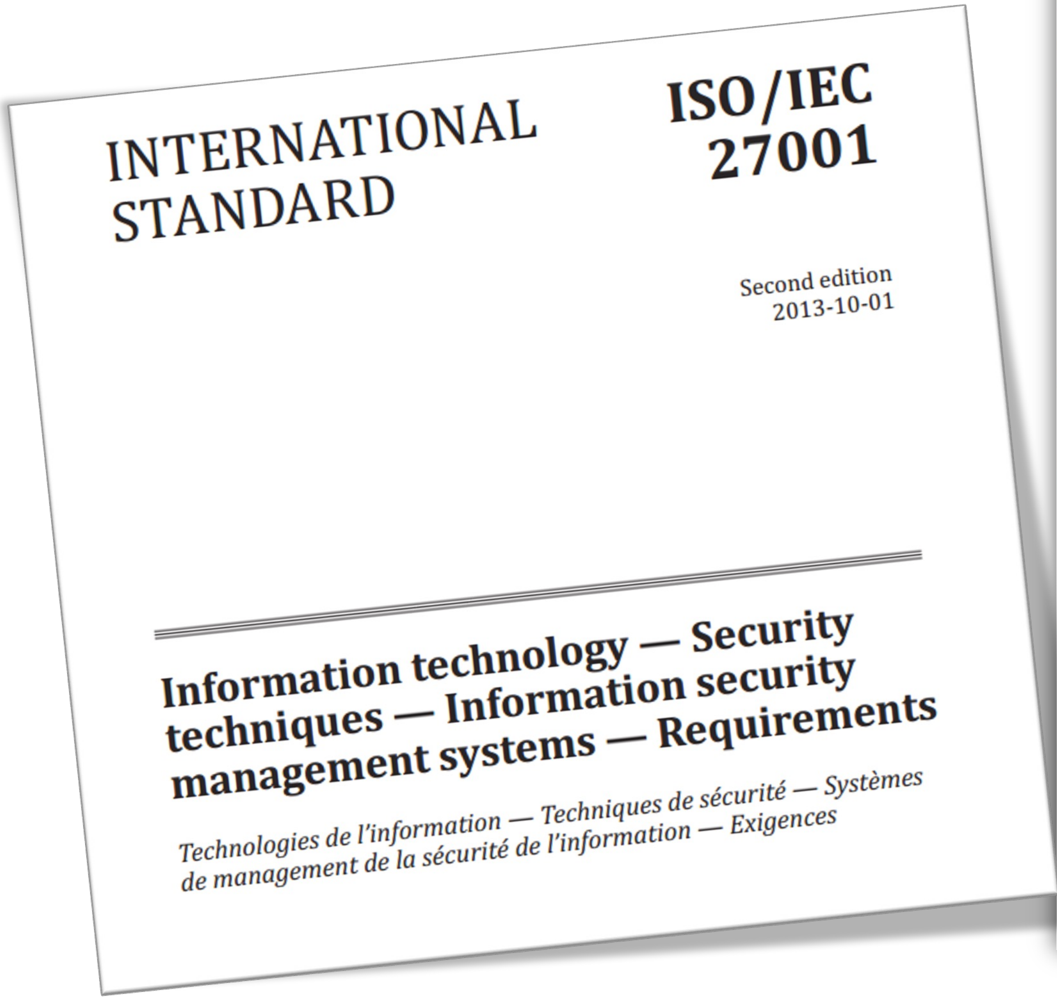
- National Vehicle Information System returns excessive vehicle owner info which are retained in Parking Database. Camera mis-calibration records biometric data that is not necessary for the service. Excessive granularity of time aids detection and singling out even if data set is otherwise transformed.

What should you – the future business leader – do, or know to ask for?

2021-04-06

Information Security Management System (ISMS)

Family of standards starting from ISO 27001



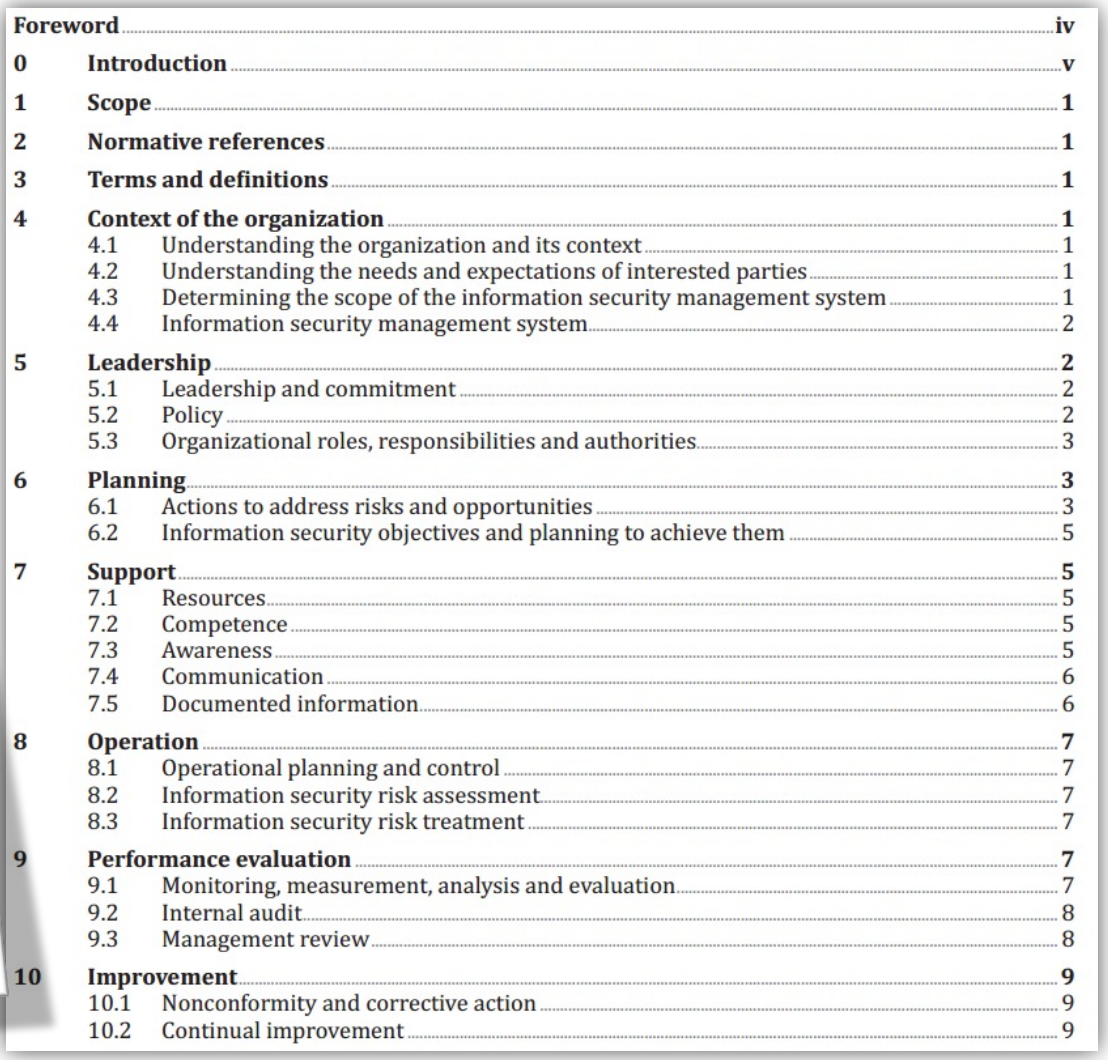
INTERNATIONAL STANDARD

ISO/IEC 27001

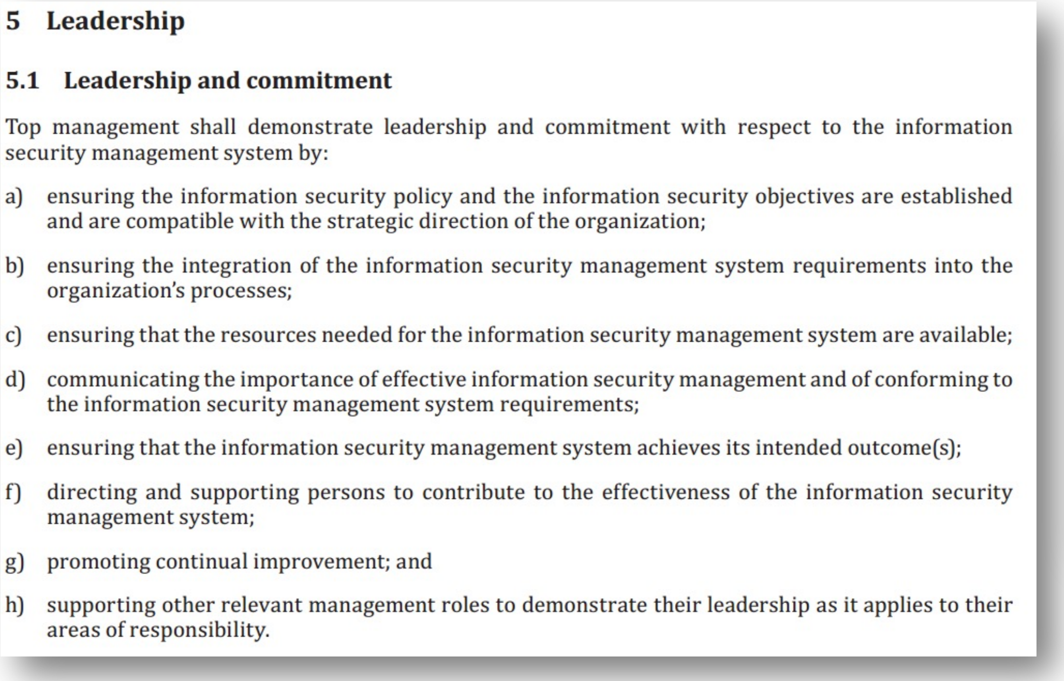
Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences



Iso 27001



5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensuring the integration of the information security management system requirements into the organization's processes;

c) ensuring that the resources needed for the information security management system are available;

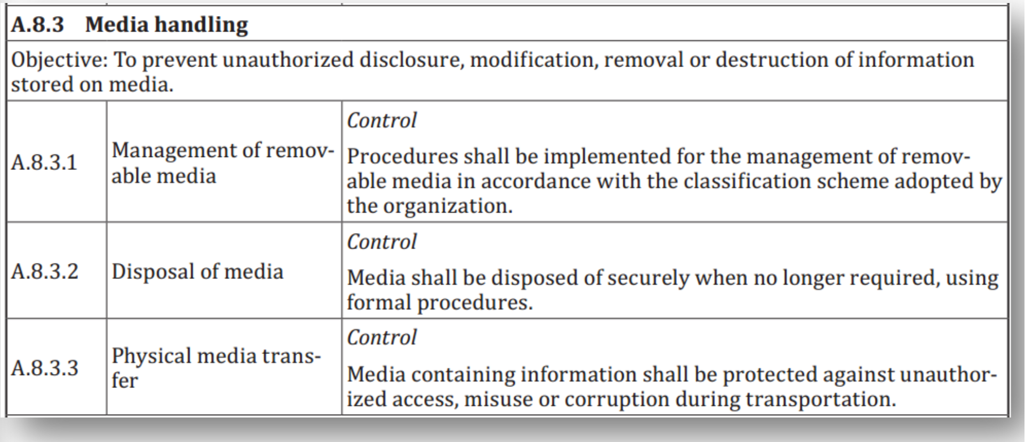
d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

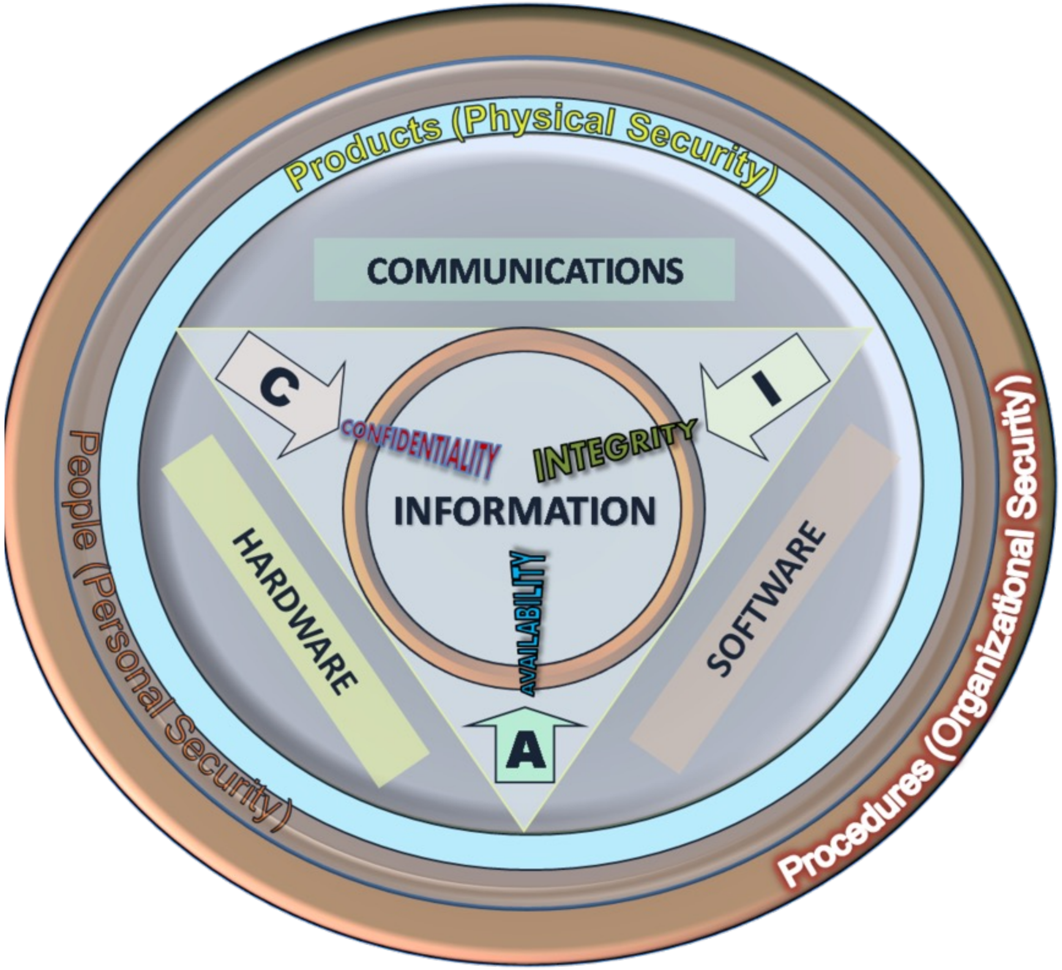
h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.



A.8.3 Media handling		
Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media	*Control* Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
A.8.3.2	Disposal of media	*Control* Media shall be disposed of securely when no longer required, using formal procedures.
A.8.3.3	Physical media transfer	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.

One definition of (Information) Security

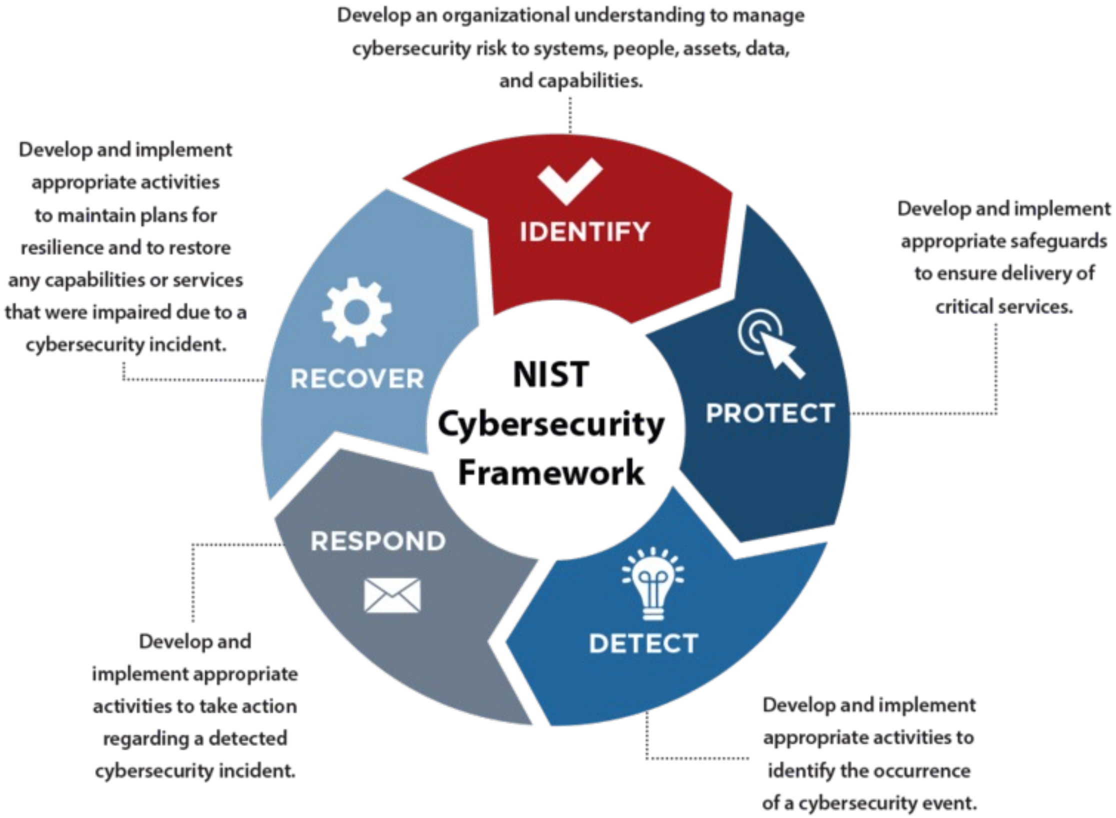
"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."
—Committee of National Security Systems, 2010


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

— Source: Wikipedia

NIST Cyber Security Framework

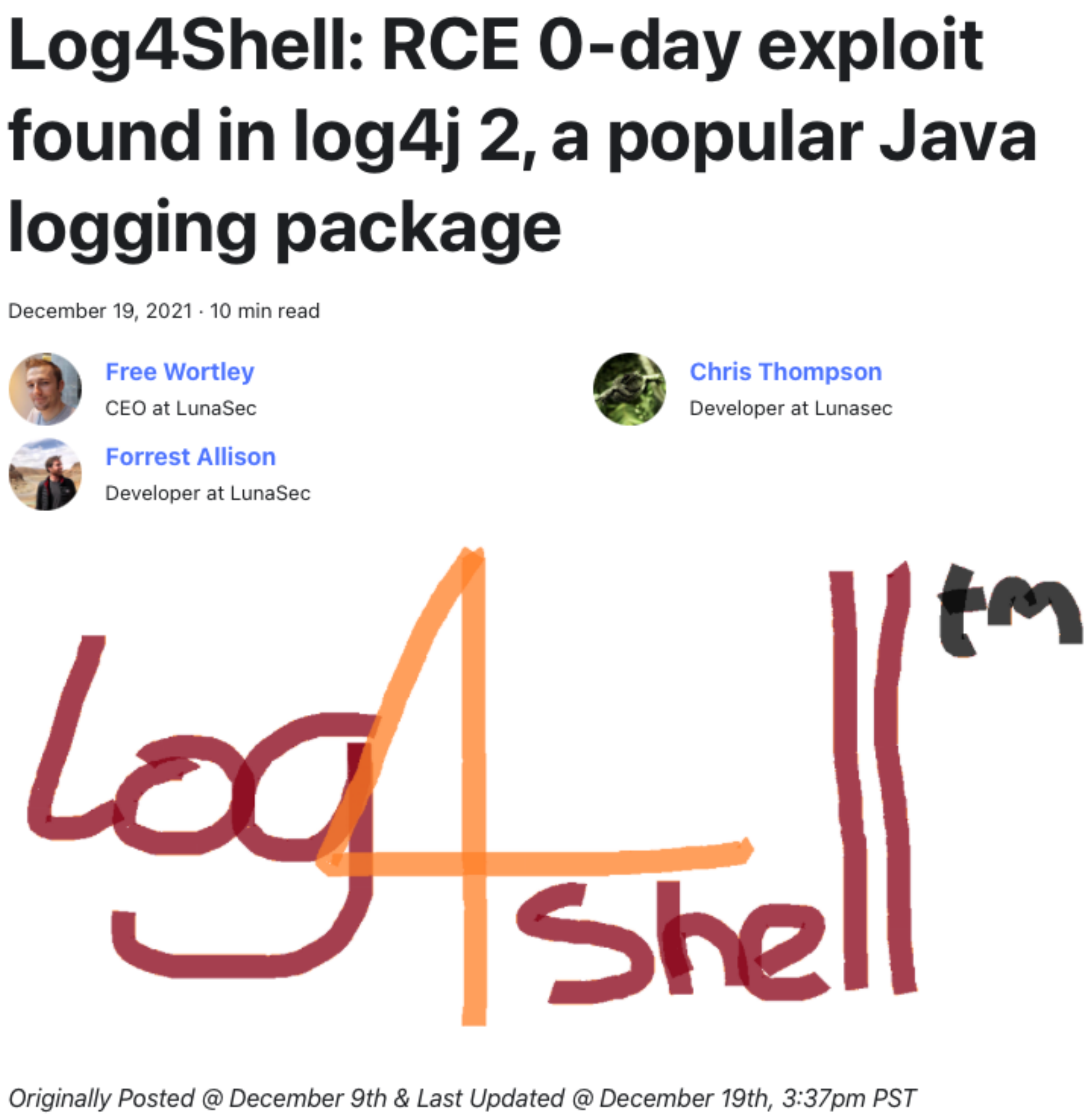
- The framework development process initiated by Executive Order 13636, February 12, 2013
- NIST CSF 1.0 public February 12, 2014
- Developed to guide critical infrastructure sectors in US
- Adopted widely by organizations and enterprises globally


Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
IDENTIFY
Develop and implement appropriate safeguards to ensure delivery of critical services.
PROTECT
Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
DETECT
Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
RESPOND
Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
RECOVER
NIST Cybersecurity Framework

Considerations for anyone to be mindful of

- Extra system comes with extra risk (hardening)
- Computers love to process data, but design shall choose what data is valid and processed, and what is disregarded (input validation)
- It would be nice if everyone could have full access, but that makes anyone a suspect in case of breach (least privilege principle)
- Every defence will fail, that’s why you want to see them in every layer (defence in depth, zero-trust)
- It’s great to have dependable employees, but you don’t want to trust all of your business on a single individual (segregation of duties)

It’s very simple, but not that easy.



Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package

December 19, 2021 · 10 min read

Free Wortley
CEO at LunaSec

Chris Thompson
Developer at Lunasec

Forrest Allison
Developer at LunaSec

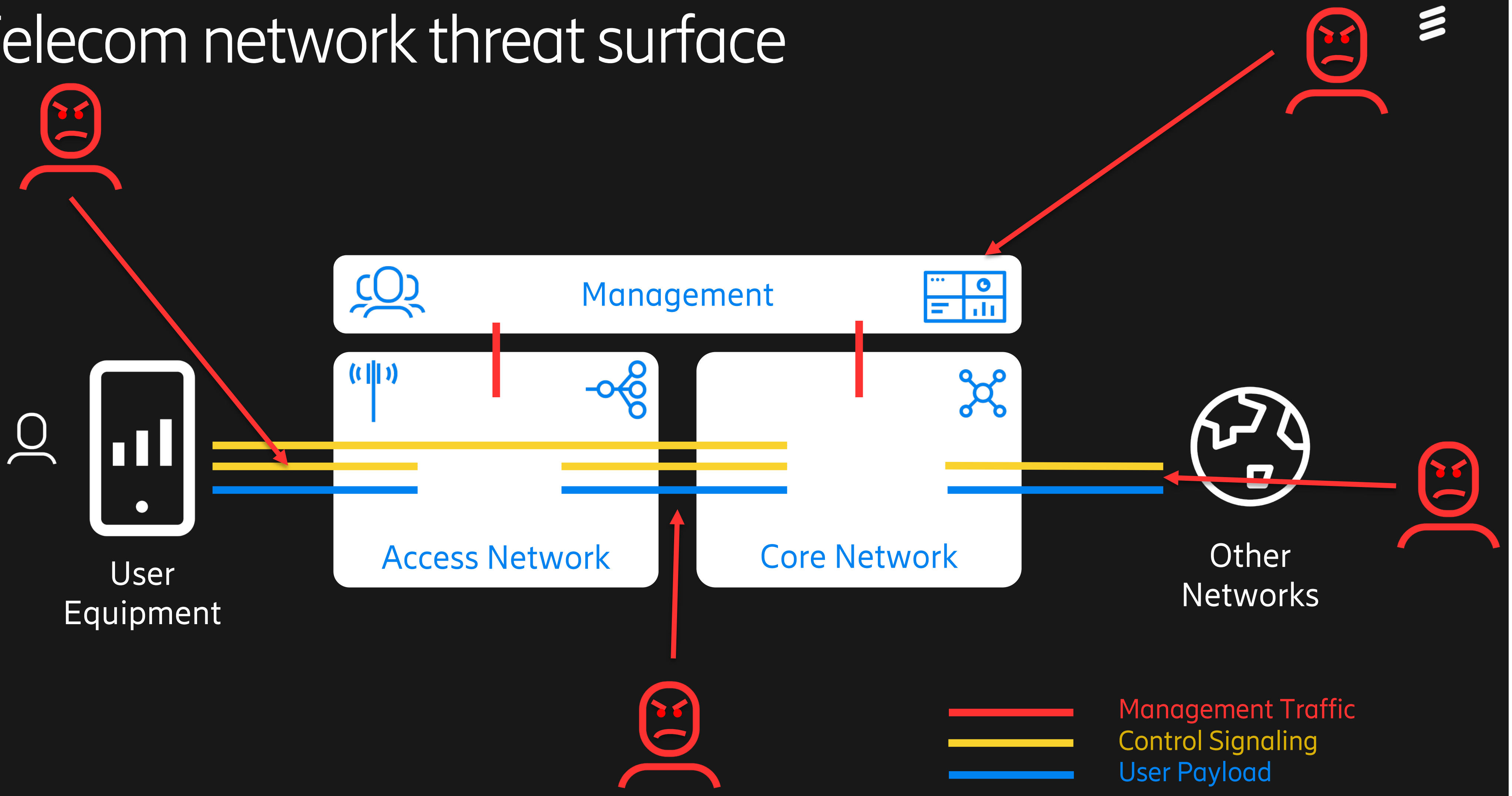
Originally Posted @ December 9th & Last Updated @ December 19th, 3:37pm PST

Other slides tbd

3GPP standard security improvements introduced in 5G (Release 15)

Subscriber authentication	Enhanced subscriber privacy	SBA security and interconnect	Integrity protection of user plane	Protection of RAN-CN interfaces (transport)
Authentication terminated in Home network Extensible authentication protocol (EAP)	Mechanism for encrypting long term subscriber identifiers Long term subscriber identifiers no longer used for paging	Support of TLS and OAuth 2.0 mandatory on all network functions Application layer security enablers between operators	Integrity protection of user plane mandatory on Device and Base station Use is optional and under the control of the operator	IPsec support mandatory on Base station side DTLS over SCTP support mandatory in addition to IPsec

Telecom network threat surface


Management
User Equipment
Access Network
Core Network
Other Networks
Management Traffic
Control Signaling
User Payload