EXCELLIUM

Your first call when it comes to IT and Security

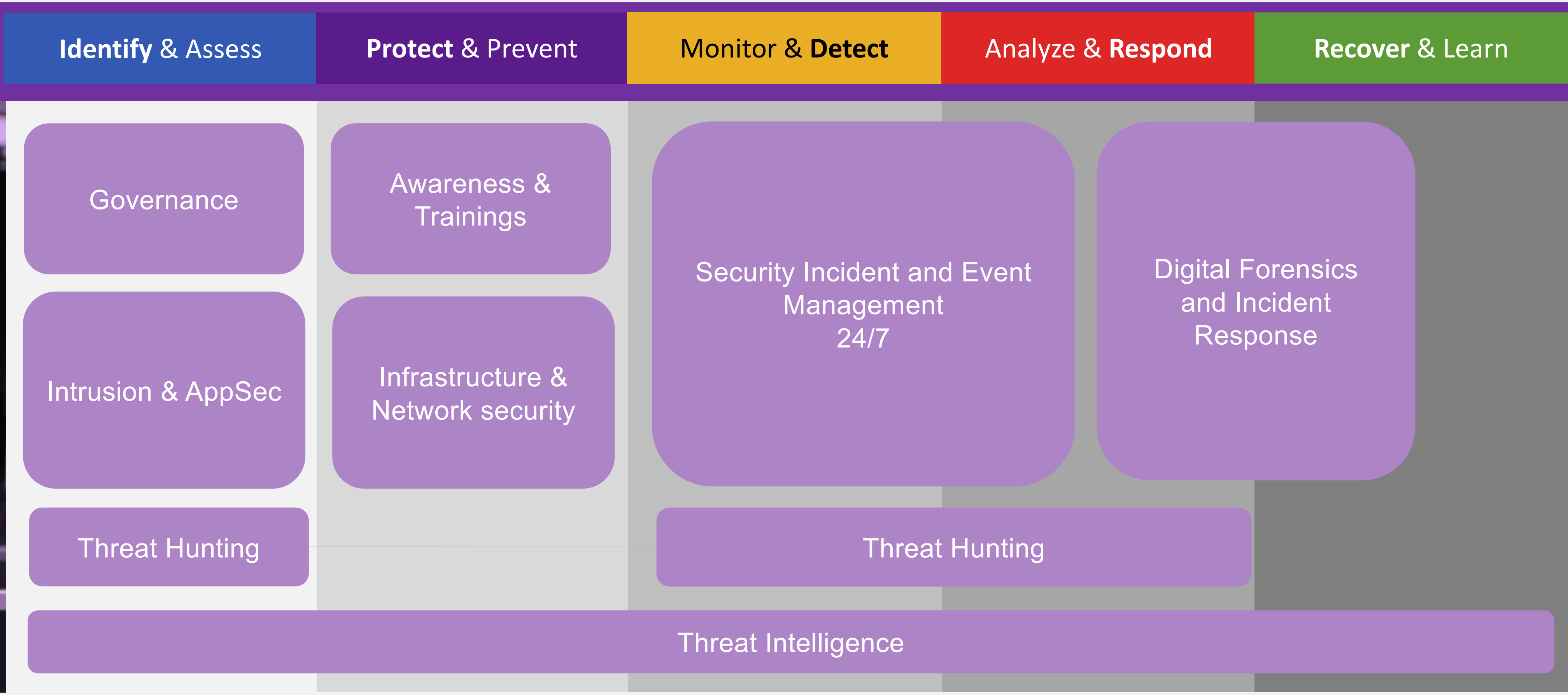
GDPR

"Enjeux et impacts au sein des équipes IT, sécurité , développement : quels sont les outils à ma disposition?"

WHAT
WE PROVIDE
Services Portfolio

Securing our customers operations to allow them running efficient and profitable business operations

Excellium is able to provide the full stack of services **from solution design to day to day operations (MSSP)**



Identify & Assess

Protect & Prevent

Monitor & **Detect**

Analyze & **Respond**

Recover & Learn

Governance

Awareness & Trainings

Security Incident and Event Management 24/7

Digital Forensics and Incident Response

Intrusion & AppSec

Infrastructure & Network security

Threat Hunting

Threat Hunting

Threat Intelligence

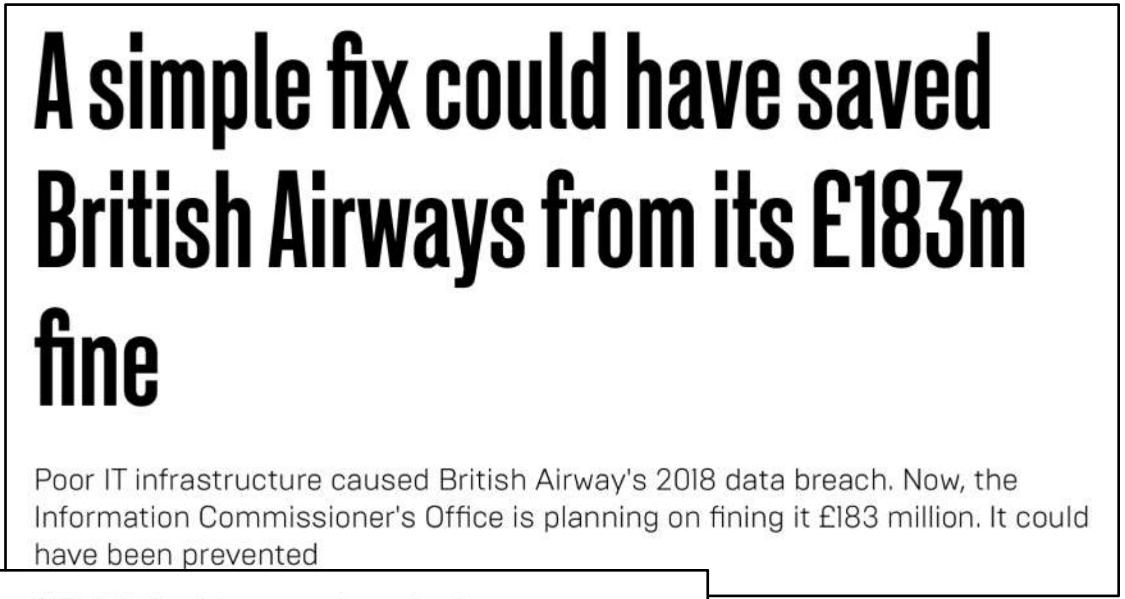
GDPR + 1 year

Good News!!!!

We don’t have anymore Data leaks

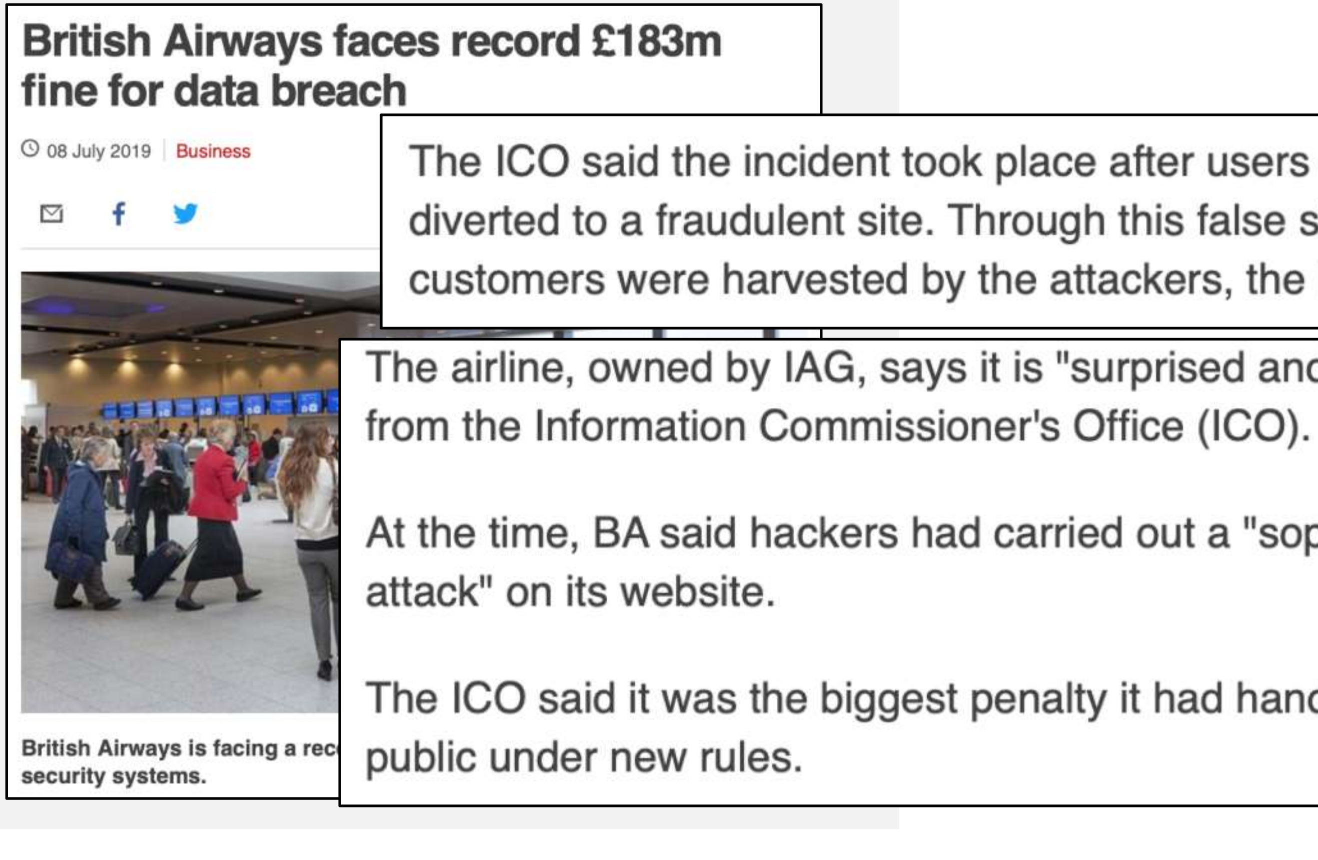
Regulation Impact

But what is the root cause?



A simple fix could have saved British Airways from its £183m fine

Poor IT infrastructure caused British Airway's 2018 data breach. Now, the Information Commissioner's Office is planning on fining it £183 million. It could have been prevented



British Airways faces record £183m fine for data breach

08 July 2019 | Business

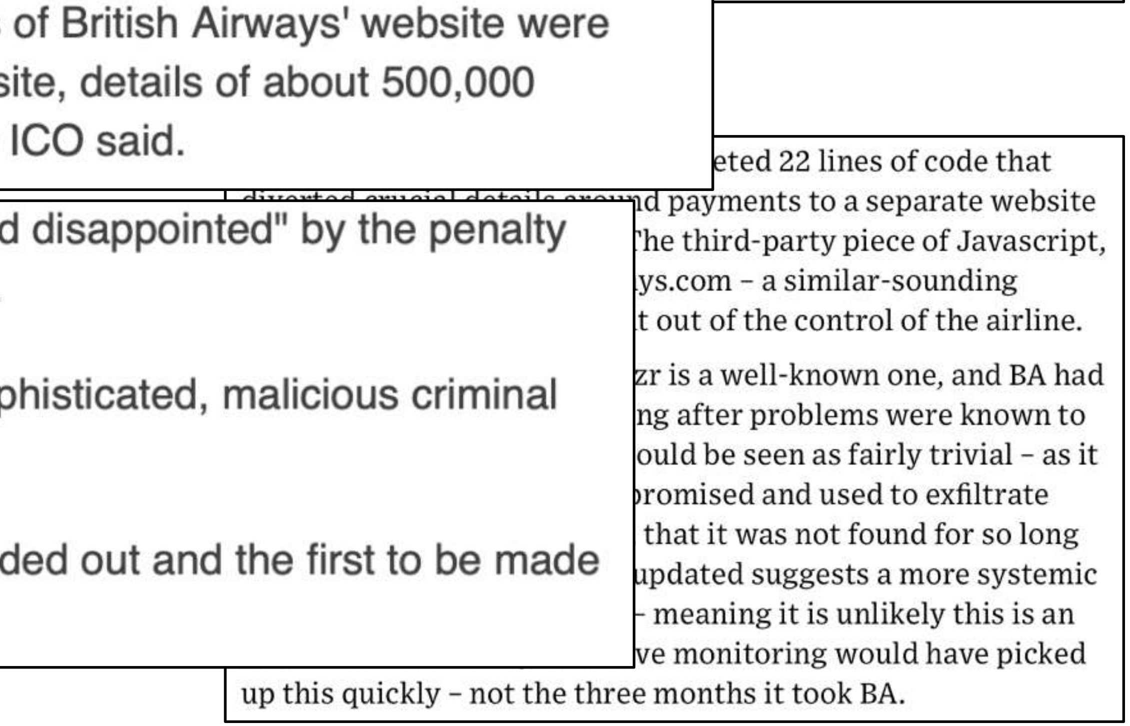
British Airways is facing a rec
security systems.

The ICO said the incident took place after users of British Airways' website were diverted to a fraudulent site. Through this false site, details of about 500,000 customers were harvested by the attackers, the ICO said.

The airline, owned by IAG, says it is "surprised and disappointed" by the penalty from the Information Commissioner's Office (ICO).

At the time, BA said hackers had carried out a "sophisticated, malicious criminal attack" on its website.

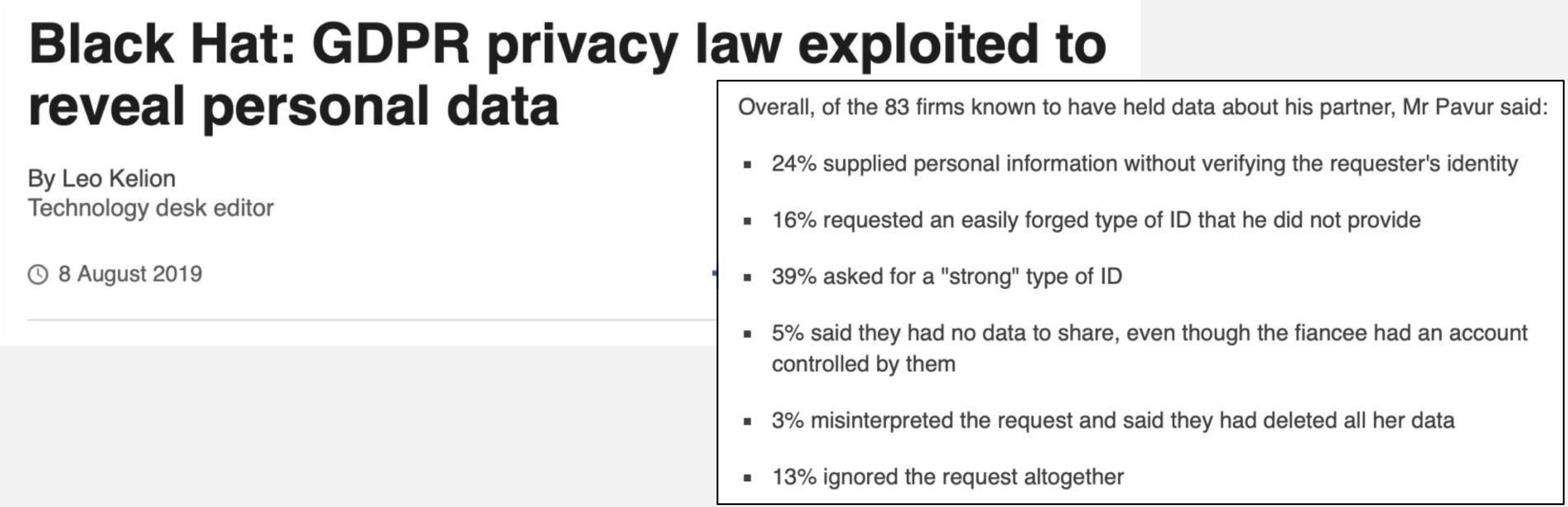
The ICO said it was the biggest penalty it had handed out and the first to be made public under new rules.



eted 22 lines of code that
diverted crucial details around payments to a separate website
The third-party piece of Javascript,
ys.com – a similar-sounding
t out of the control of the airline.

zr is a well-known one, and BA had
ng after problems were known to
ould be seen as fairly trivial – as it
promised and used to exfiltrate
that it was not found for so long
updated suggests a more systemic
– meaning it is unlikely this is an
ve monitoring would have picked
up this quickly – not the three months it took BA.

GDPArrrrr: Using Privacy Laws to Steal Identities



Black Hat: GDPR privacy law exploited to reveal personal data

By Leo Kelion
Technology desk editor

8 August 2019

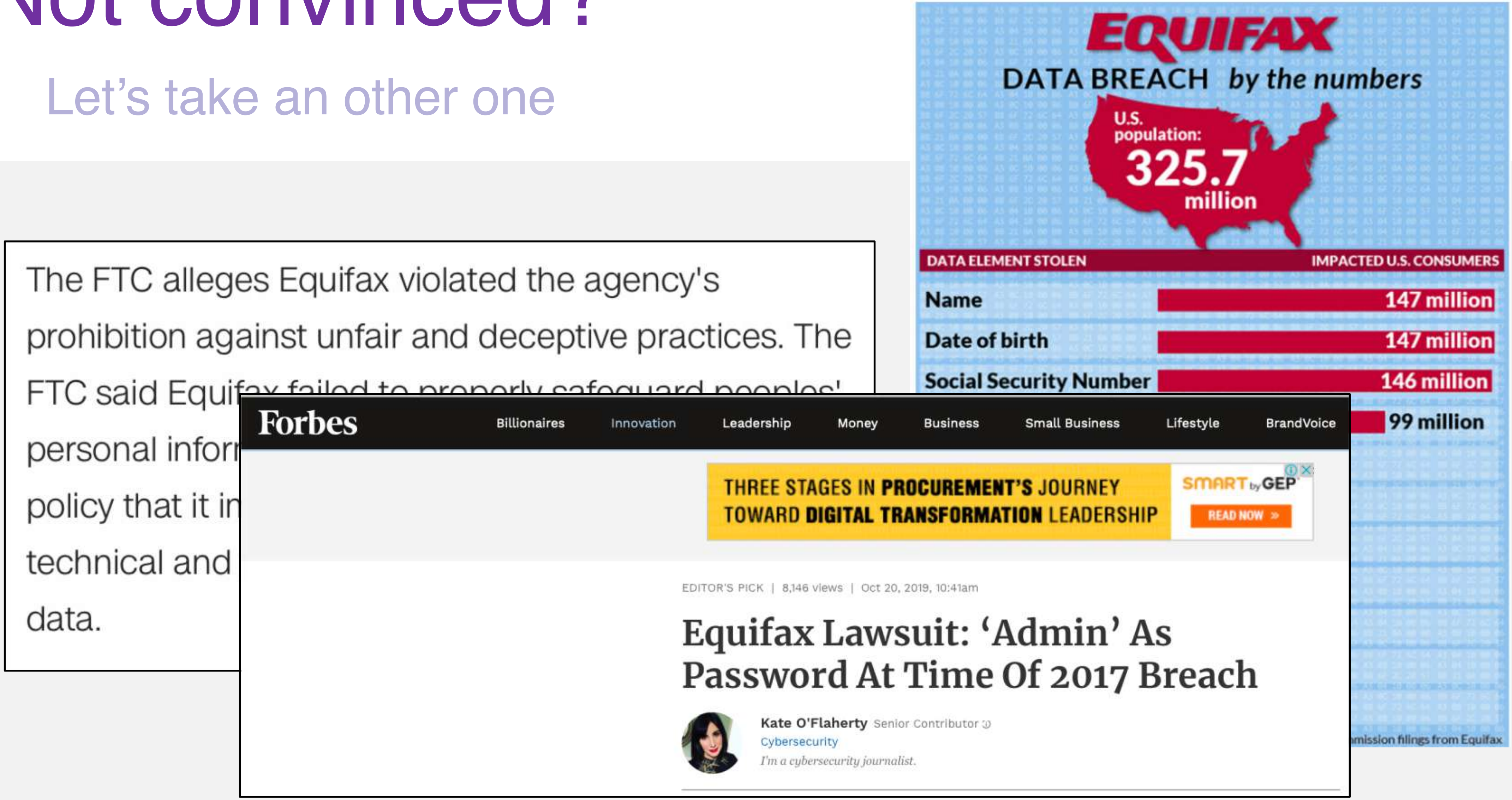
Overall, of the 83 firms known to have held data about his partner, Mr Pavur said:

- 24% supplied personal information without verifying the requester's identity
- 16% requested an easily forged type of ID that he did not provide
- 39% asked for a "strong" type of ID
- 5% said they had no data to share, even though the fiancee had an account controlled by them
- 3% misinterpreted the request and said they had deleted all her data
- 13% ignored the request altogether

https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf

Not convinced?

Let’s take an other one



The FTC alleges Equifax violated the agency's prohibition against unfair and deceptive practices. The FTC said Equifax failed to properly safeguard peoples' personal infor

policy that it in

technical and

data.

EQUIFAX

DATA BREACH *by the numbers*

U.S. population: 325.7 million

DATA ELEMENT STOLEN	IMPACTED U.S. CONSUMERS
Name	147 million
Date of birth	147 million
Social Security Number	146 million
	99 million

mission filings from Equifax

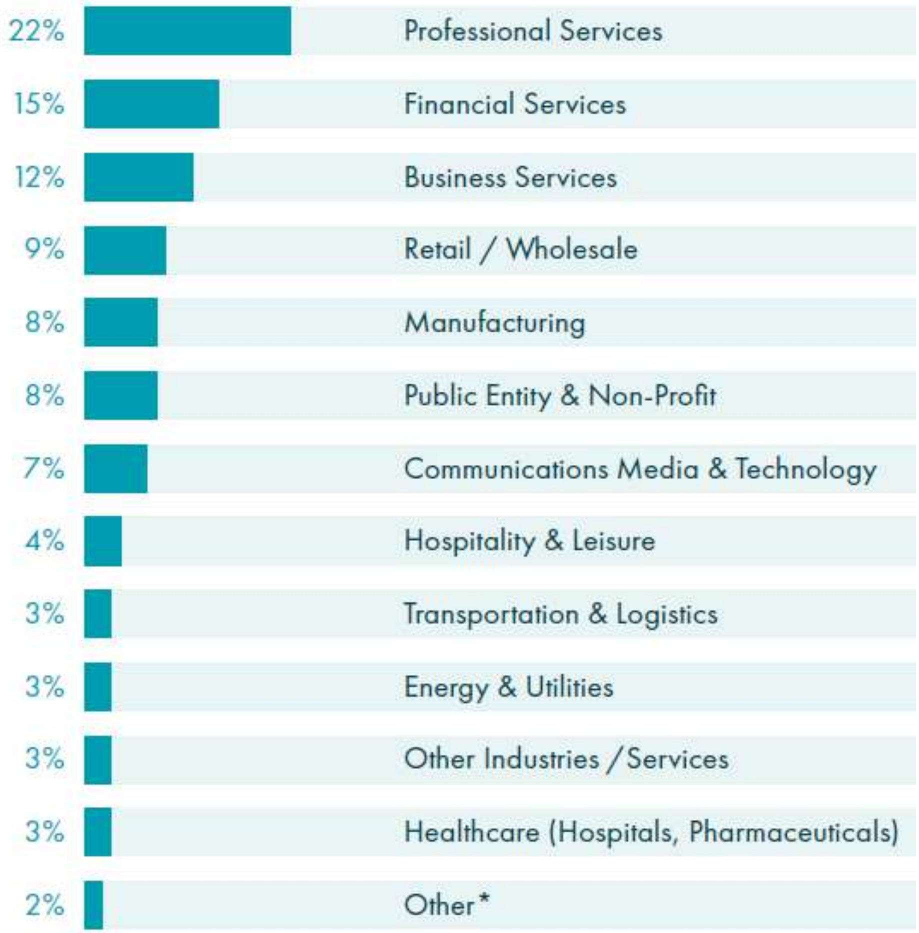
EDITOR'S PICK | 8,146 views | Oct 20, 2019, 10:41am

Equifax Lawsuit: ‘Admin’ As Password At Time Of 2017 Breach

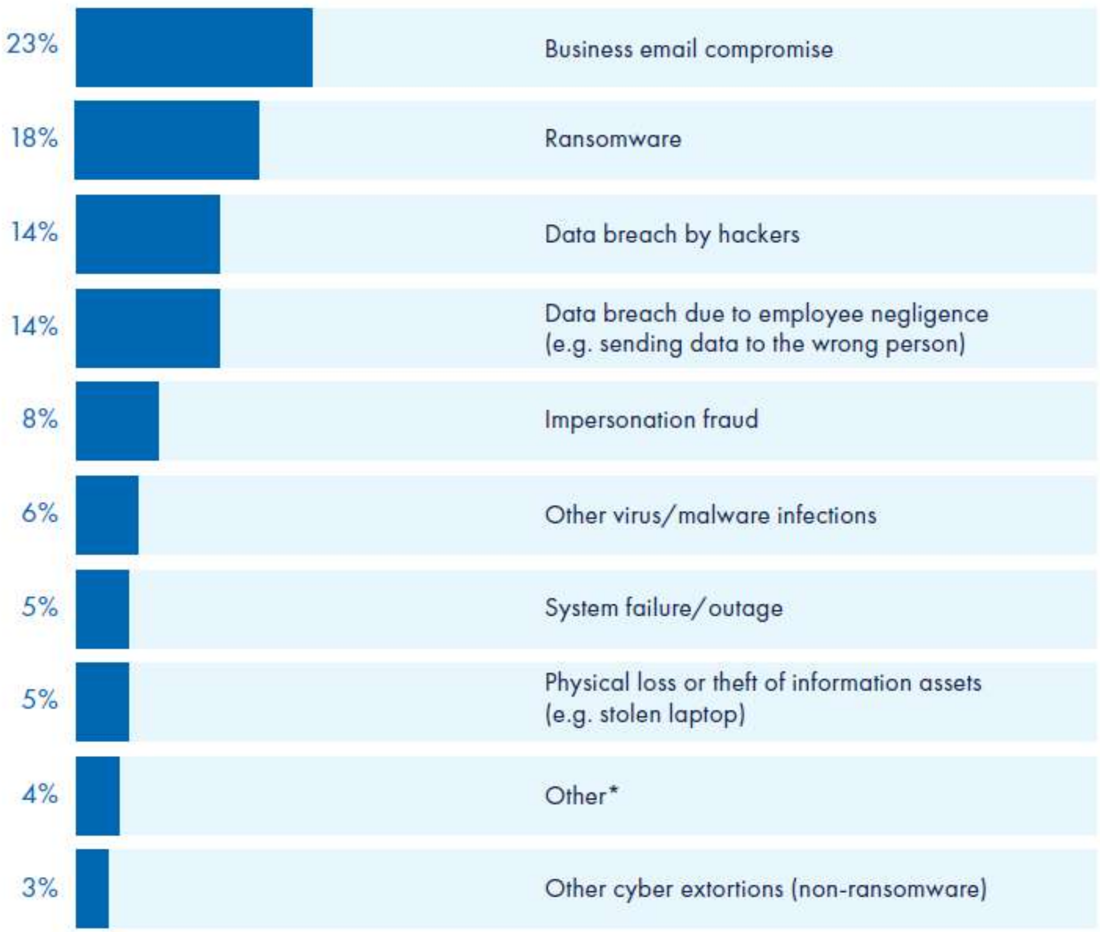
Kate O'Flaherty Senior Contributor
Cybersecurity
I'm a cybersecurity journalist.

Cyber Claims - EMEA 2018

By Industry / Reported incidents



*Food & Beverage, Construction, Education



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

Where are the basics?

Let’s talk 2 minutes

GDPR

- Privacy compliance
- Data Security

NIS

- Resilience compliance
- Data Security

PCI-DSS

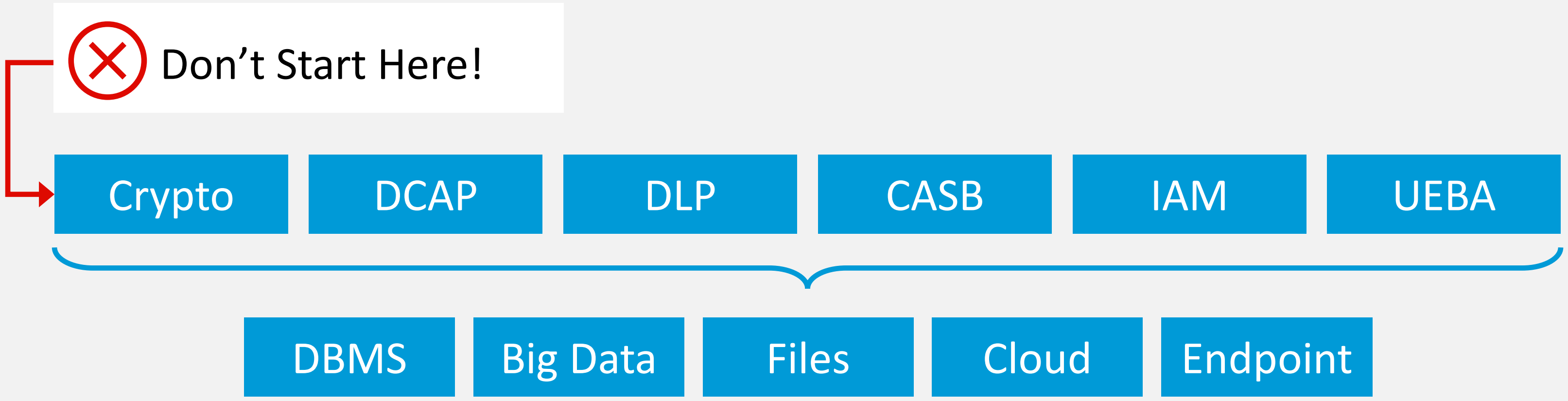
- Credit Card complaince
- Data Security

?? Compliance = Security ??

What are the Prime factors ???

Data Security Governance

Source Gartner



Don’t Start Here!

Crypto | DCAP | DLP | CASB | IAM | UEBA

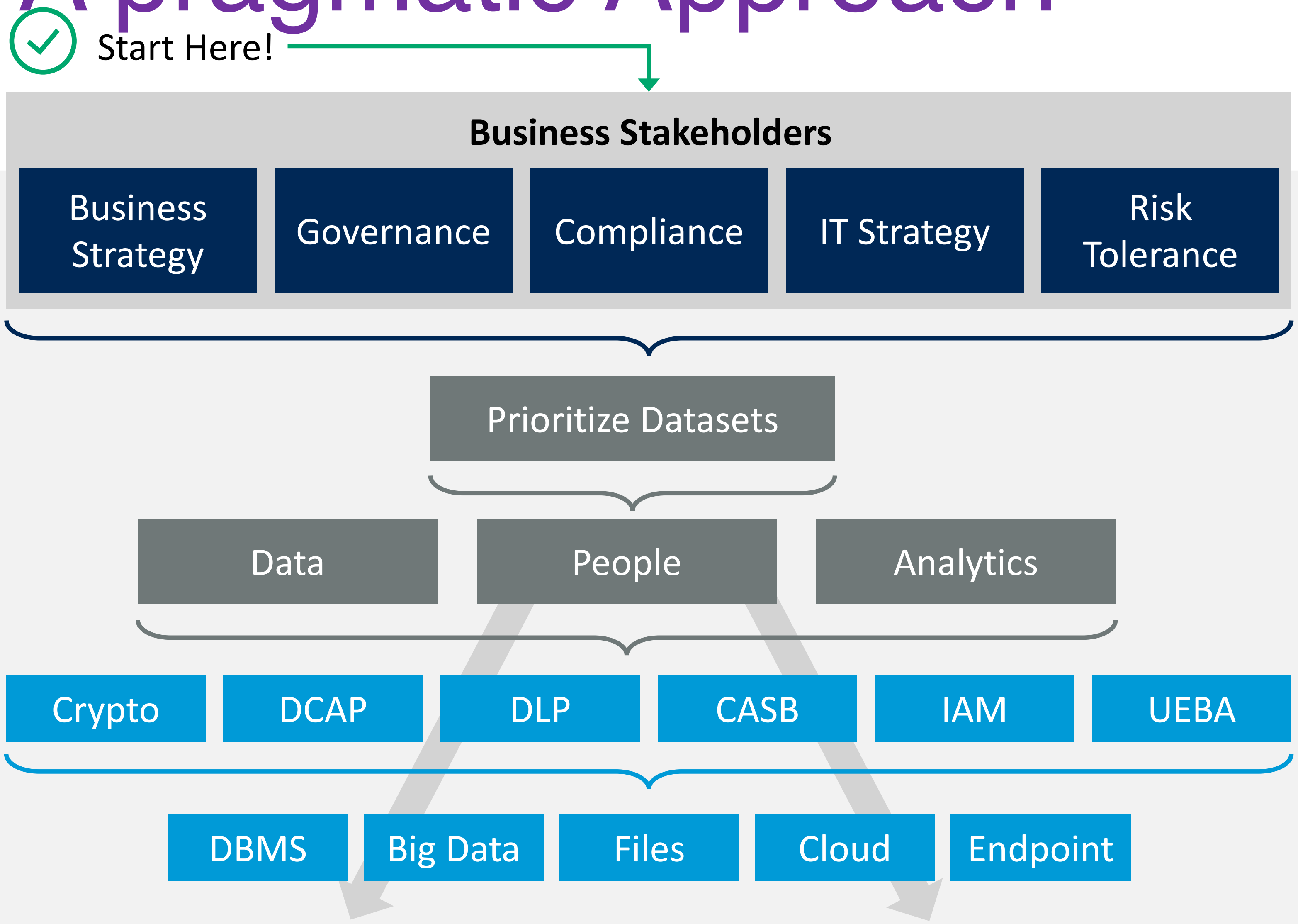
DBMS | Big Data | Files | Cloud | Endpoint

4 Implement Security Products

5 Orchestrate Policies for **All** Products

A pragmatic Approach

Source Gartner



✓ Start Here!

Business Stakeholders

Business Strategy

Governance

Compliance

IT Strategy

Risk Tolerance

Prioritize Datasets

Data

People

Analytics

Crypto

DCAP

DLP

CASB

IAM

UEBA

DBMS

Big Data

Files

Cloud

Endpoint

1 Balance Business Needs Versus Risks

✕ But Don't stop there!

2 Identify, Prioritize and Manage Dataset Life Cycles

3 Define Data Security Policies

4 Implement Security Products

5 Orchestrate Policies for **All** Products

CHALLENGES & OPPORTUNITIES

> **“Cyber Security has been approach from a technology point of view where it is in fact a question of risk management”**

4 keys constraints

Skills & resources
Shortage create strong issue for most of the major players

Cyber Incidents
Happening on a daily basis creating a C level topic & a resiliency concern

Digitalization
Increase the exposed lanscape (mobility, IoT, smart, automation …)

Regulations
Constant pressure on the economic actors (eg.GDPR, PCI DSS, PSD 2)

IT Leadership agenda

Data valuation
Exploiting "data" capital to boost competitiveness

Mobility
Security and standardization of the user experience

Devops
Faced with the need to accelerate "time to market" and gain agility

Digitalization
API
IoT & smart devices
Blockchain
Microservices…

GLOBAL ACTION PLAN

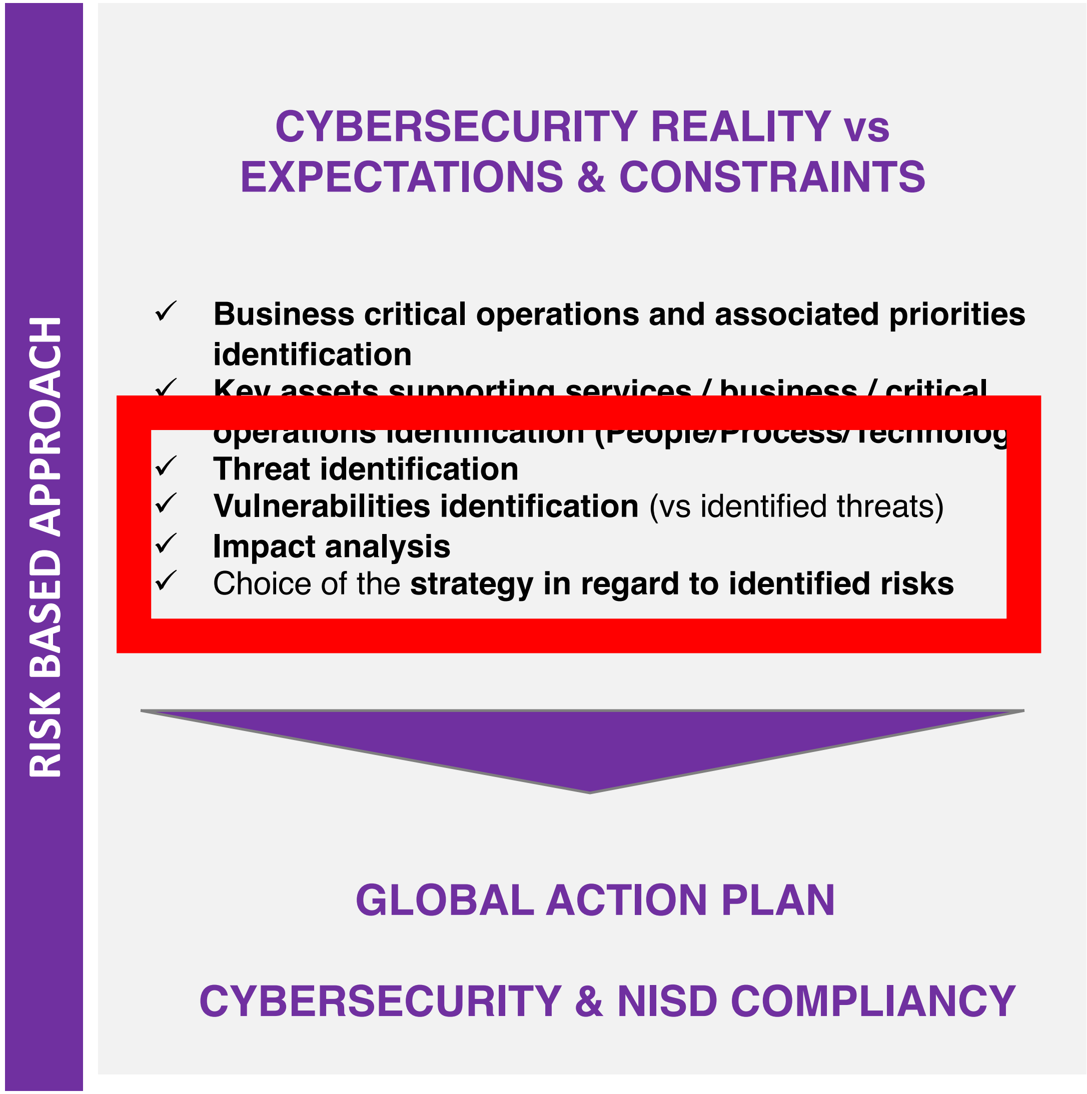
Security initiatives examples

A pragmatic Approach

In 8 steps

- What is your actual posture? (leverage your DRP/BCP works, GDPR analysis, …recents audits or pentest results, …) in order to define the actual level of maturity against the threat landscape;
- What is the adequate level of maturity (needed) (considering the ecosystem) ;
- Definition of your risk profile (which threats, scenarios, …);
- Based on that what is your technical capability to address such scenarios;
- Crisis management implementation and testing;
- Are you able to react?
- So what do you need to monitor?
- Let’s now challenge your current security operations and controls.

Excellium Resilience Risk Based Approach



RISK BASED APPROACH

CYBERSECURITY REALITY vs EXPECTATIONS & CONSTRAINTS

- ✓ **Business critical operations and associated priorities identification**
- ✓ **Key assets supporting services / business / critical operations identification (People/Process/Technolog**
- ✓ **Threat identification**
- ✓ **Vulnerabilities identification** (vs identified threats)
- ✓ **Impact analysis**
- ✓ Choice of the **strategy in regard to identified risks**

GLOBAL ACTION PLAN

CYBERSECURITY & NISD COMPLIANCY

Inline with

- ✓ **the NIS Directive** related to measures to ensure a common high level of security of networks and information systems in the Union
- ✓ **The Belgian and Luxembourg law** - Law establishing a framework for the security of networks and information systems of general interest for public security
- ✓ The guidelines and recommendations of the Enisa
- ✓ Cybersecurity best practise acquired by Excellium long experience and expertise

Collection of evidences on security measures for NISD

Excellium' approach

ASSESSMENT GOVERNANCE/ PEOPLE/ PROCESS /TECHNOS

Interviews – Collection of documents

Usage of the recommended framework Mapping depending on the industry from ENISA (e.g. ISO27001/NIST/CIS
For NISD compliance Assessment)

"WP2017 O-1-1-1-1 Mapping of OES Security Requirements to Specific Sectors"

- ISO27001 ; CIS top20 ; NIST CSF; PSD2
- Bespoke Security framework
- Or very specific standard related to the sector

STEP 1

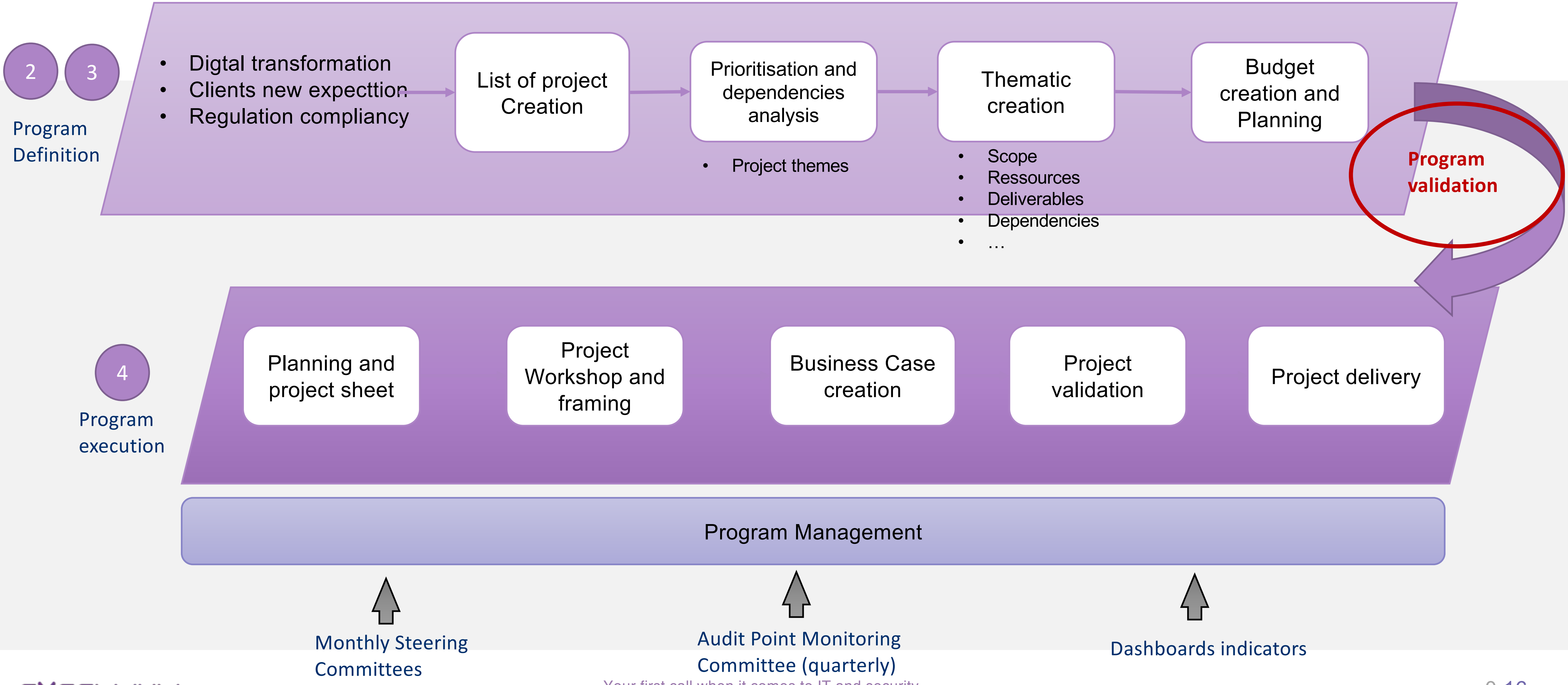
Control validation / Configuration reviews e.g.

❑ WP-REVUE D'ARCHITECTURE	Consultancy expertise
❑ WP-REVUE DE CONFIGURATION	Consultancy expertise CIS benchmark
❑ WP-REVUE ADMINISTRATION (AD)	PingCastle–Active Directory Audit
❑ WP-REVUE DES VULNERABILITES	Qualys Scans
❑ WP-REVUE DOMAIN DNS	EyeTLD
❑ WP-REVUE ANTI DDOS & TEST DDOS	DDoS Testing -MazeBolt
❑ WP-PENTEST	Pentester assessment
❑ WP Mail/Web flow SC validation	CSOC Cymulate
❑ WP-APPsec validation	Appsec expert assessment
❑ … INPUT FROM CLIENT	ANY relevant tech assessment

STEP 2

RBA INPUTS

Security Maturity Program Definition/creation/Execution



2

3

Program Definition

- Digtal transformation
- Clients new expecttion
- Regulation compliancy

List of project Creation

Prioritisation and dependencies analysis

- Project themes

Thematic creation

- Scope
- Ressources
- Deliverables
- Dependencies
- …

Budget creation and Planning

Program validation

4

Program execution

Planning and project sheet

Project Workshop and framing

Business Case creation

Project validation

Project delivery

Program Management

Monthly Steering Committees

Audit Point Monitoring Committee (quarterly)

Dashboards indicators

Maturity assessment

Key steps

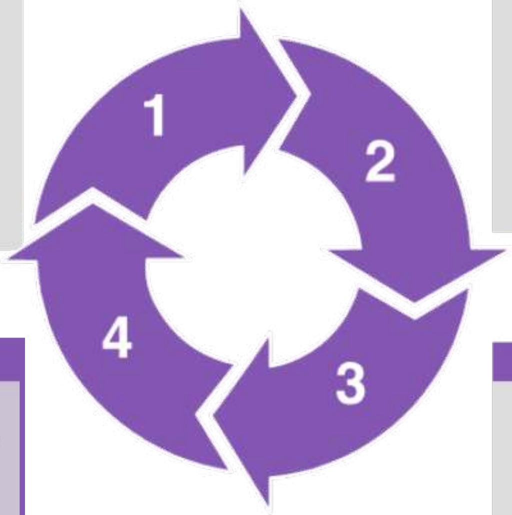
To keep in mind:

- Reassessment allows to **update maturity level of the organization** and adapt the cybersecurity program.
- Alignment of controls is essential to ensure the **consistency** between the framework and the evolution of the organization’s context.
  - **Context evolution** can be due to evolution of the organization’s strategy, legal and regulatory requirements, business objectives or services provided.
  - **Reassessment** should be performed if any context evolution has impacted the framework and related controls.

1 - Initiate

Choose a **framework** with regard to your **organization’s context**.

Assess and formalize information security **maturity level** of your organization.



2 - Coordinate

Identify and prioritize **key aspects to improve**.

Define and align your **cybersecurity program** according to the prioritization.

3 - Validate

Validate and confirm during and at the end of a project that **information security objectives** are met.

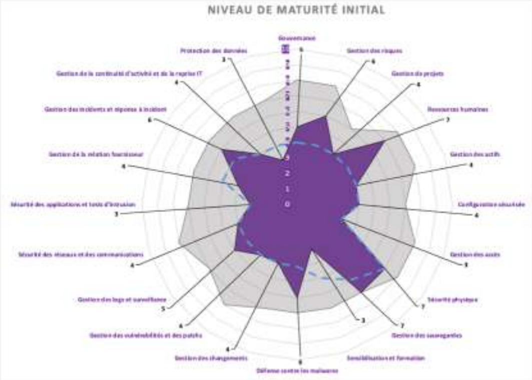
4 - Monitor

Update maturity level according to the cybersecurity program **evolution**.

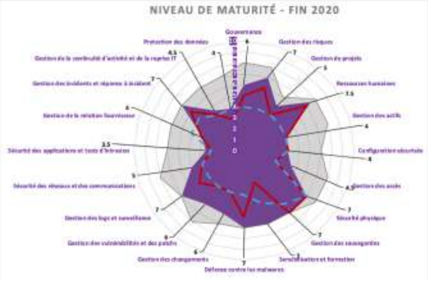
Review and align controls of the framework in accordance with your context.

Maturity Level definition

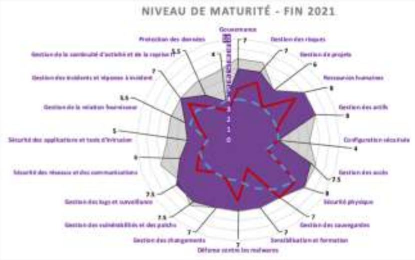
From « **As Is** » to « **To Be** »



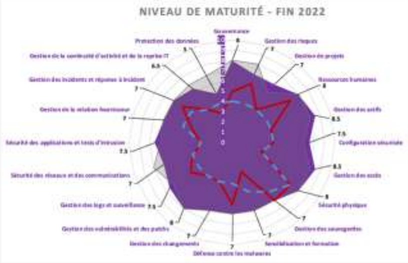
Existing



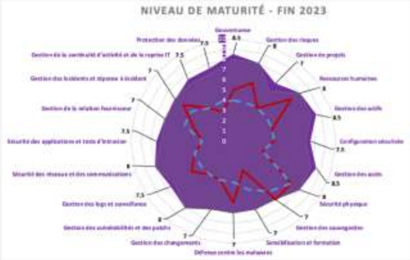
End of 2020



End of 2021



End of 2022



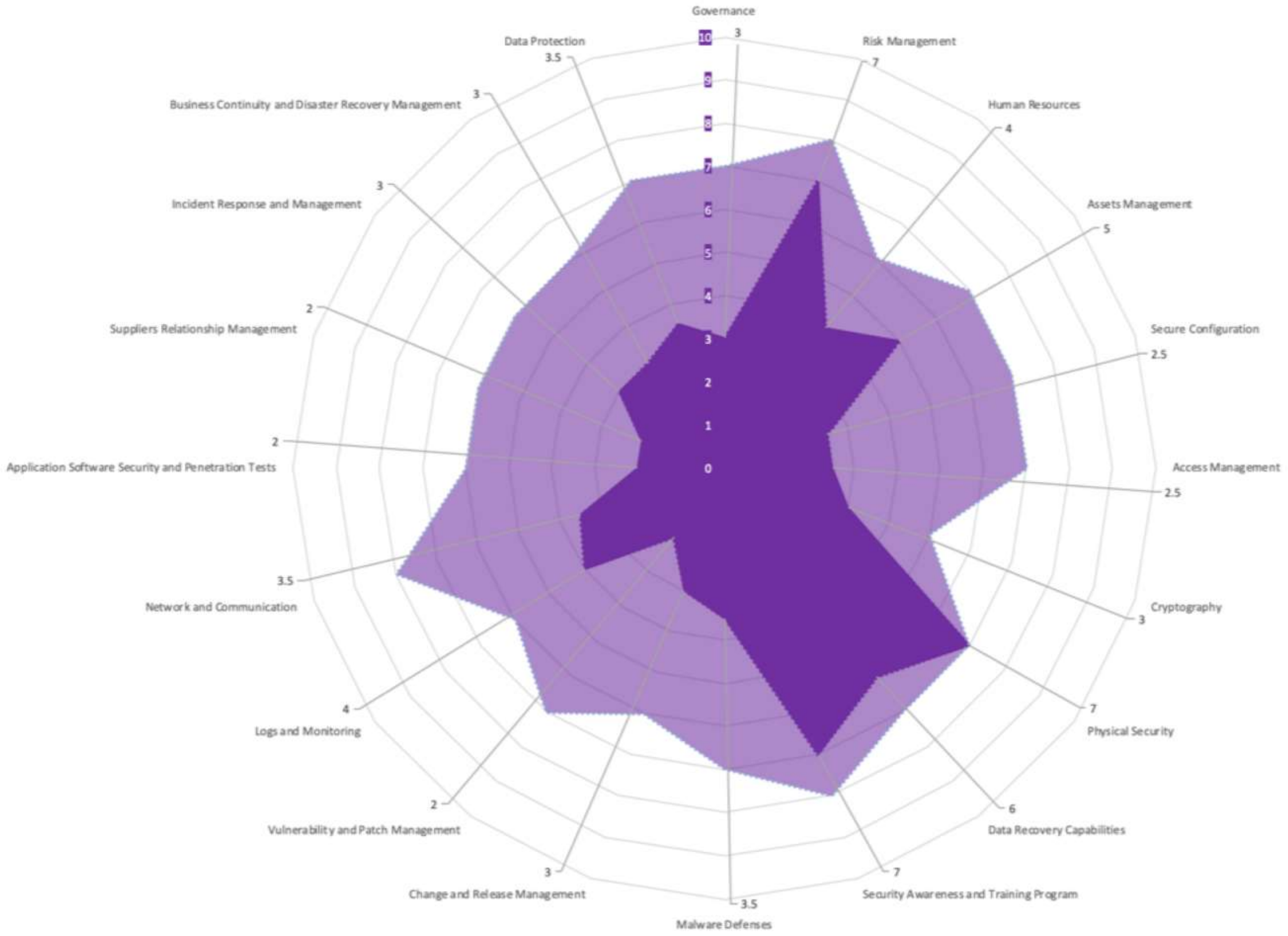
End of 2023

2019 → **End 2023**

Maturity level

Initial state

INITIAL MATURITY LEVEL



Security Initiatives

Security Initiatives	Description
Patch Management	Deal with vulnerabilities, define and deploy patch management to remediate identified flaws.
Privileged Account Management	Management of privileged accounts life cycle (technical accounts, e.g. administration accounts, service accounts, generic accounts)
Logs Management	Identification of attributes/activities to log, centralization into a SIEM, logs review.
Vulnerability Management	Assets scoping, vulnerabilities classification, remediation rules.
IAM	Management of identity and access rights.
Configuration Management	Hardening, process for maintaining configuration and security baselines.
Network Security	Global actions regarding network weaknesses (traffic, security issues, etc.).
Network Security - Firewall	Firewall security issues remediation (CISCO, SOPHOS).
Network Security - Email	IronPort security issues remediation.
Network Security - Load Balancer	Load Balancer (Citrix Netscaler) security issues remediation.
Network Security - Web Gateway	Web Gateway (McAfee) security issues remediation.
Network Security - SSL VPN	VPN SSL security issues remediation.
Virtualization	ESX security issues remediation.
Windows	Windows server security issues remediation.
Assets Management	Inventory of assets, active scanning tool, USB keys lifecycle management.
Software Management	Whitelist of software, restrictions on software installation.

Security Initiatives

Security Initiatives	Description
Network Security - Web Browser	Web browser security issues remediation.
Malware Protection	Implementation and management, including follow-up of events, of malware protection solution on all devices.
Backup Management	Backup management and restoration process (testing).
Data Protection	Data classification, DLP.
Network Security - Wifi	Wifi security issues remediation.
Awareness and Training	Awareness program, standard and specific trainings about information security.
Application Security	SDLC, code testing.
IT Services Management	Request and incident management, release management, change management.
Penetration Tests	Penetration tests program.
Authentication	Authentication mechanisms, including MFA.
PKI	PKI management, including certificates lifecycle.
Supplier Management	Suppliers selection process, suppliers monitoring process.
Human Resources	Review of HR processes and practices.
Governance	Project management, policies, KPI, internal audit, procedures formalization.
Business Continuity	BIA, BCP/DRP procedures, testing program.

Projets actuellement en cours non considérés dans l'évaluation de maturité :

- *Revue de la politique de sécurité*
- *Programme de sensibilisation*
- *Définition du Cyber response plan*
- *Intégration de la sécurité dans les projets*
- *SAM*
- *Déploiement CISCO ASA*

Niveau de maturité initial

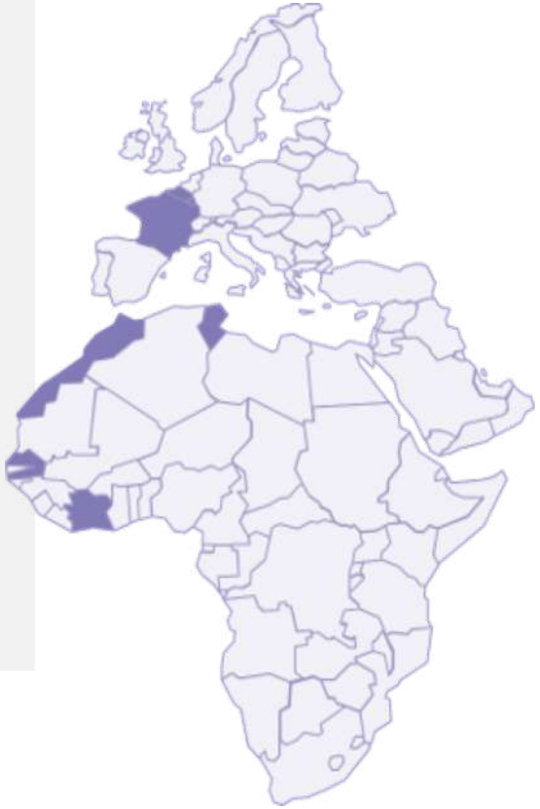
Thématiques	Niveau de maturité initial
Gouvernance	**5**
Gestion des risques	**6**
Gestion de projets	**4**
Ressources humaines	**7**
Gestion des actifs	**4**
Configuration sécurisée	**4**
Gestion des accès	**3**
Sécurité physique	**7**
Gestion des sauvegardes	**7**
Sensibilisation et formation	**3**
Défense contre les malwares	**6**
Gestion des changements	**4**
Gestion des vulnérabilités et des patchs	**4**
Gestion des logs et surveillance	**5**
Sécurité des réseaux et des communications	**4**
Sécurité des applications et tests d'intrusion	**3**
Gestion de la relation fournisseur	**4**
Gestion des incidents et réponse à incident	**6**
Gestion de la continuité d'activité et de la reprise IT	**4**
Protection des données	**3**

Définition de **20 thématiques** s'appuyant sur des **référentiels reconnus** pour établir le niveau de maturité sur base **des exigences normatives** (ISO 27001, SANS CIS 20) et **des risques encourus** (voir mapping).

WHO WE ARE

Excellium launched its services in Belgium, and work with subsidiaries active in Morocco, Tunisia, Senegal and Ivory Coast, France and Switzerland are planned for 2019.

6	**Awards** (IBM 2014-2016-2017-2018) APSI (2017) ITONE (2018)
15.4	A **turnover** of about 15,4 M€ in 2018
30	Technical Partnerships
100	Cyber security **specialists**
180	**Clients** (financial, multinational and governmental organizations)



LUXEMBOURG
Excellium Services
CSC, Datacenter Lux, CGI, Fujitsu

BELGIUM
Excellium Services BE
NRB & Telenet (320M€ & Revenues)

SENEGAL
Suricate Solution
ADIE (National IT agency)

TUNISIA
Excellium Factory - Alfaros
Tunisie Telecom

FRANCE
Jaguar Networks

SWISS

MOROCCO
MedTech Group