Da una protezione perimetrale ad una user centric

Security Summit 2019 - Treviso

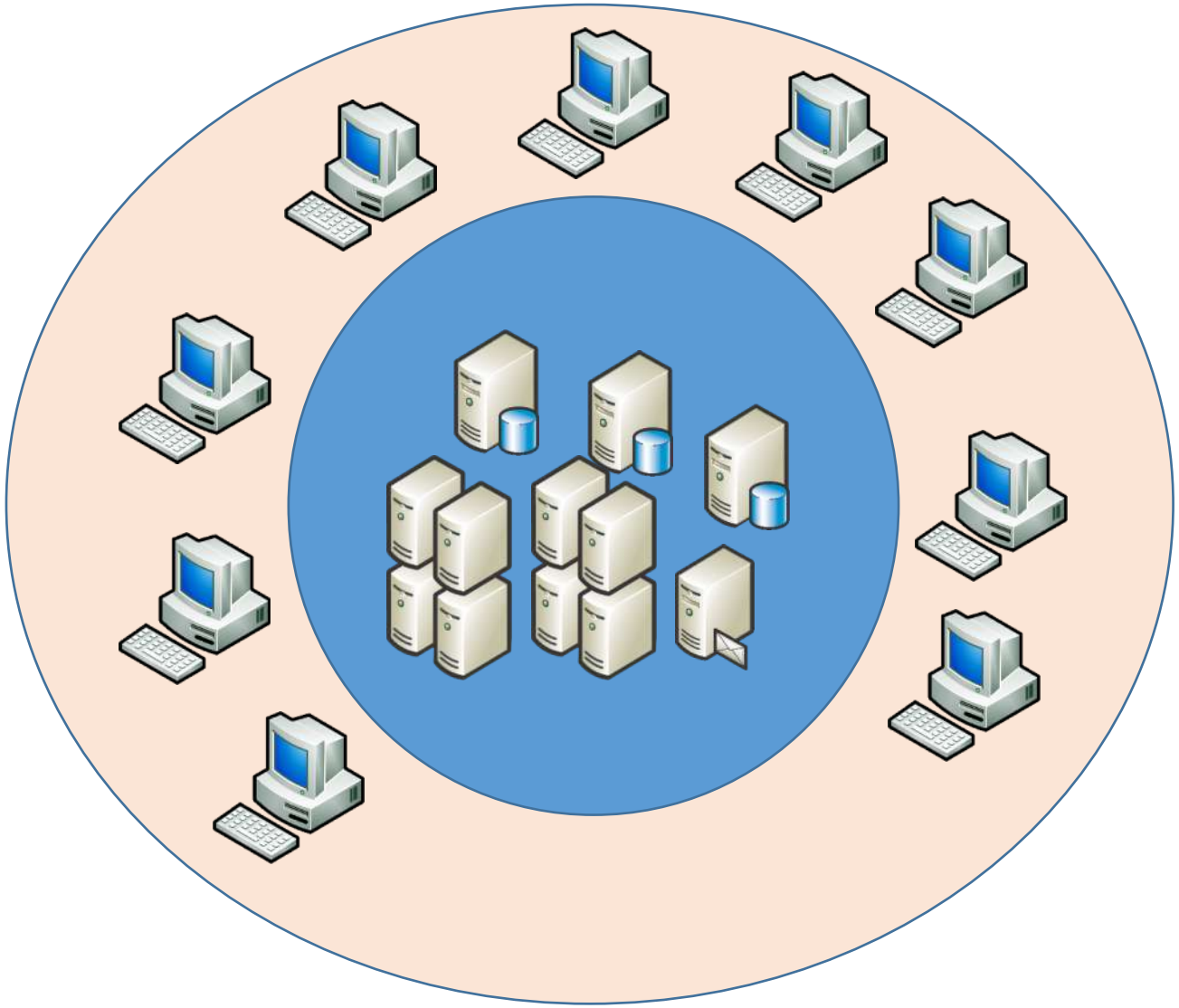
AXSYM SRL Corso Porta Nuova, 109 - 37122 Verona, Italia
P.IVA/C.F. 04446280234 Tel. +39 045 5118570 - www.axsym.it - info@axsym.it

Axsym è una realtà giovane che offre servizi legati alla Governance IT e alla Cyber Security

Le informazioni sono il principale patrimonio che le organizzazioni dovrebbero preoccuparsi di proteggere

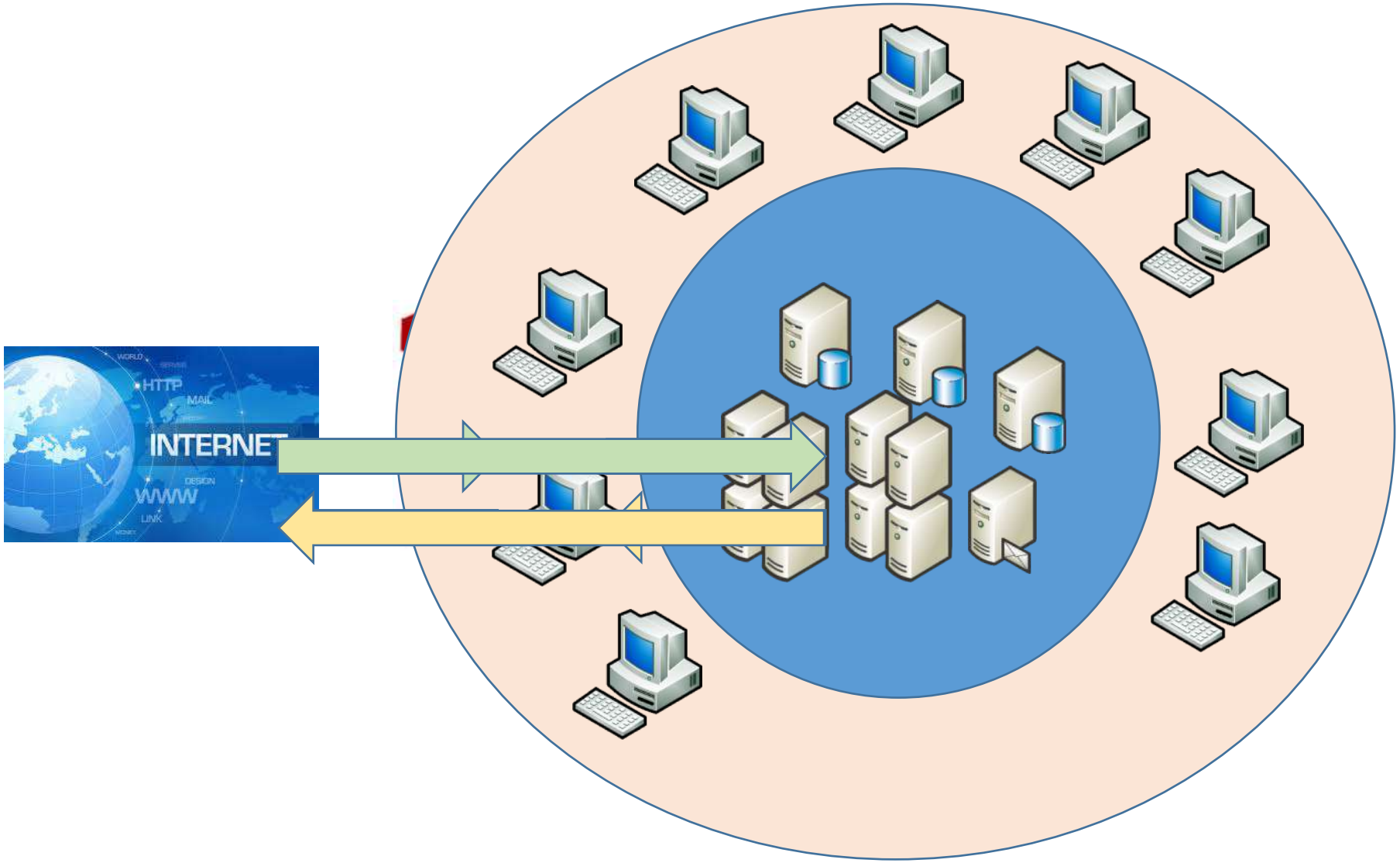
Per molti anni l'approccio utilizzato dalle aziende era piuttosto «semplice»

L'approccio



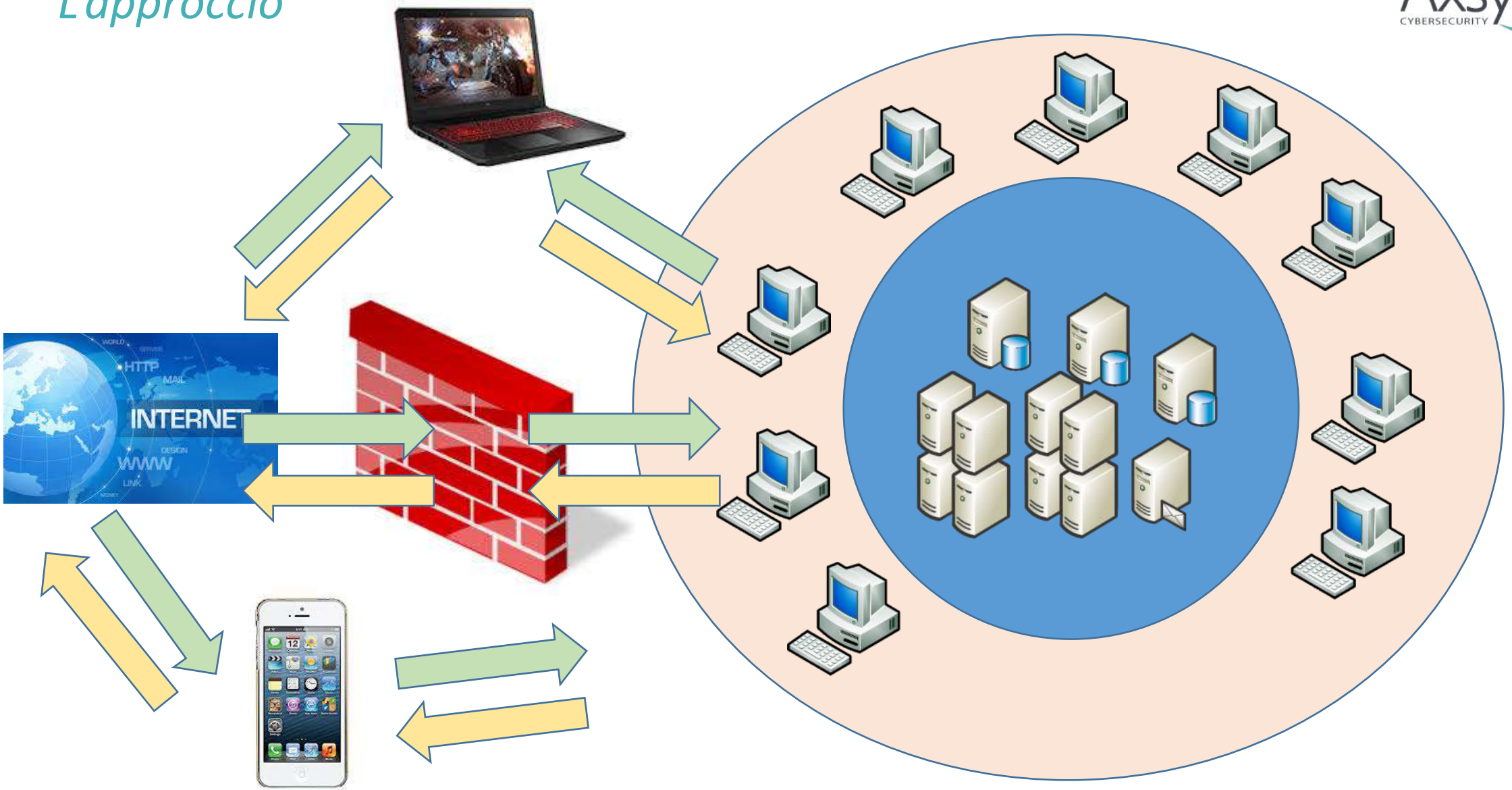
L'approccio

L'approccio



L'approccio

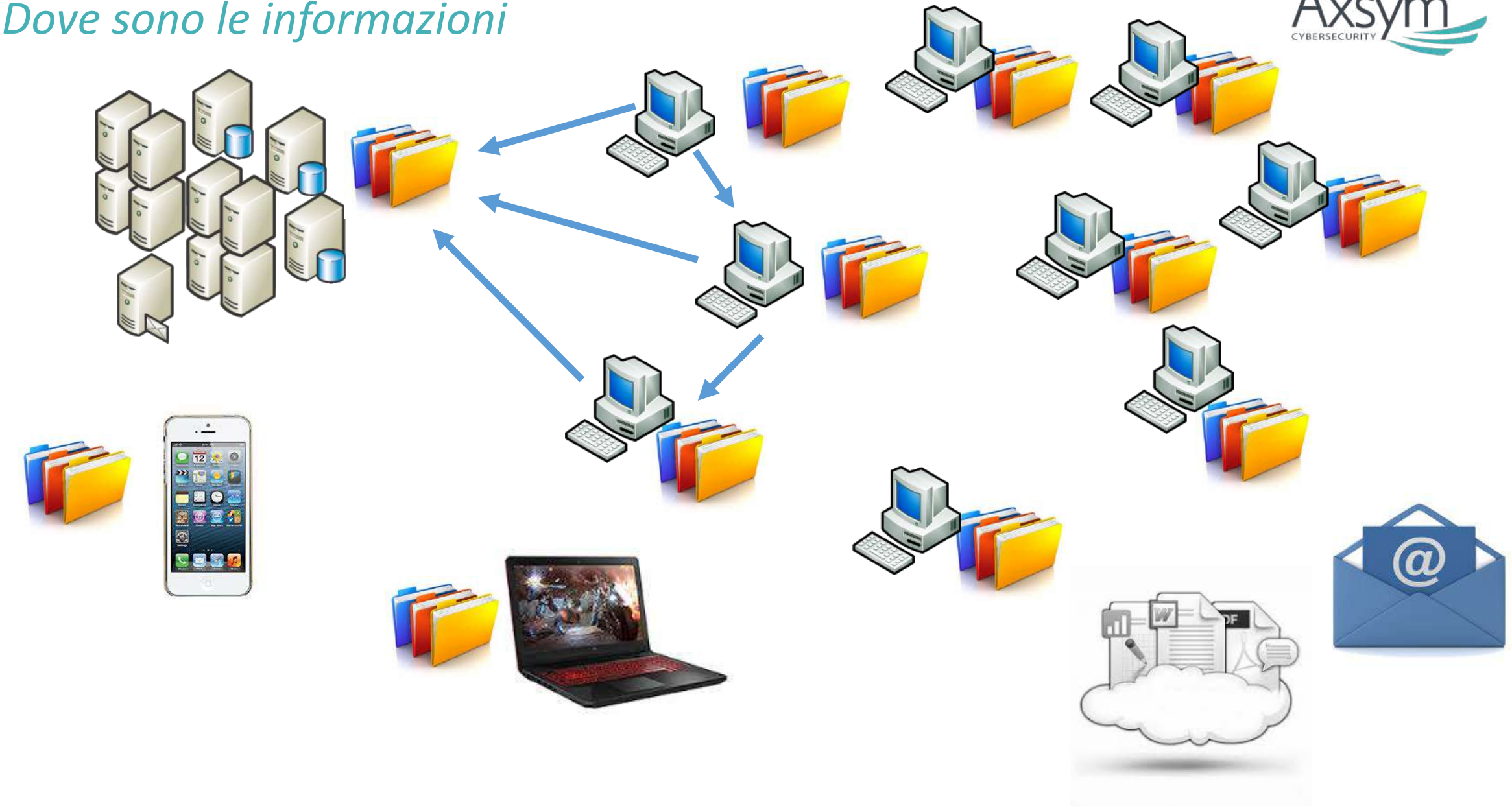
L'approccio



Qual è oggi il perimetro?

Dove sono le mie informazioni?

Dove sono le informazioni



Quando si utilizza il cloud, chi gestisce la sicurezza?

Ma di chi è la responsabilità per le informazioni?

Il GDPR chiarisce che senza dubbio la responsabilità è del Titolare

Al di là delle informazioni personali, pensiamo anche ai dati di business

Possiamo affidare la responsabilità delle nostre informazioni ad una terza parte?

Qual è la posizione fisica dei dati in cloud?

La posizione fisica dei dati determina il tipo di normativa applicabile

La posizione fisica dei dati determina anche il tipo di sorveglianza, che in alcuni paesi potrebbe essere diverso da quanto ci si aspetta

L’azienda che usa di servizi in cloud mantiene il controllo sull’accesso alle informazioni

Ma è sempre e sicuramente così?

Quali sono le procedure adottate dal fornitore in caso di disastro o in caso di Data Breach?

Non essendoci più un perimetro così definito, la protezione delle informazioni richiede qualche riflessione

Difficile che informazioni critiche siano trasmesse a qualcuno fuori dall'organizzazione

Ma quando trasmetto via email delle informazioni critiche ad un collega?

E se il collega scarica la posta elettronica su uno smartphone?

E se lo smartphone non è aziendale?

La perdita di un dispositivo contenente informazioni personali accessibili può configurarsi come Data Breach

Questo è l'aspetto più legato alla normativa

Ma le informazioni di business?

Non necessariamente dobbiamo pensare a brevetti o simili

È sufficiente pensare al CRM, alla lista clienti

Partiamo sempre da un presupposto di buona fede e fedeltà degli utenti

Ma se non fosse sempre così?

Qual è il ruolo dell'IT?

Spesso nelle aziende l'IT è «invisibile»

Ci si accorge dell'esistenza dell'IT solo quando qualcosa non funziona

All'IT vengono delegate le più disparate incombenze

Gestione dotazioni aziendali

Gestione della sicurezza delle informazioni

Formazione sull'uso degli strumenti IT

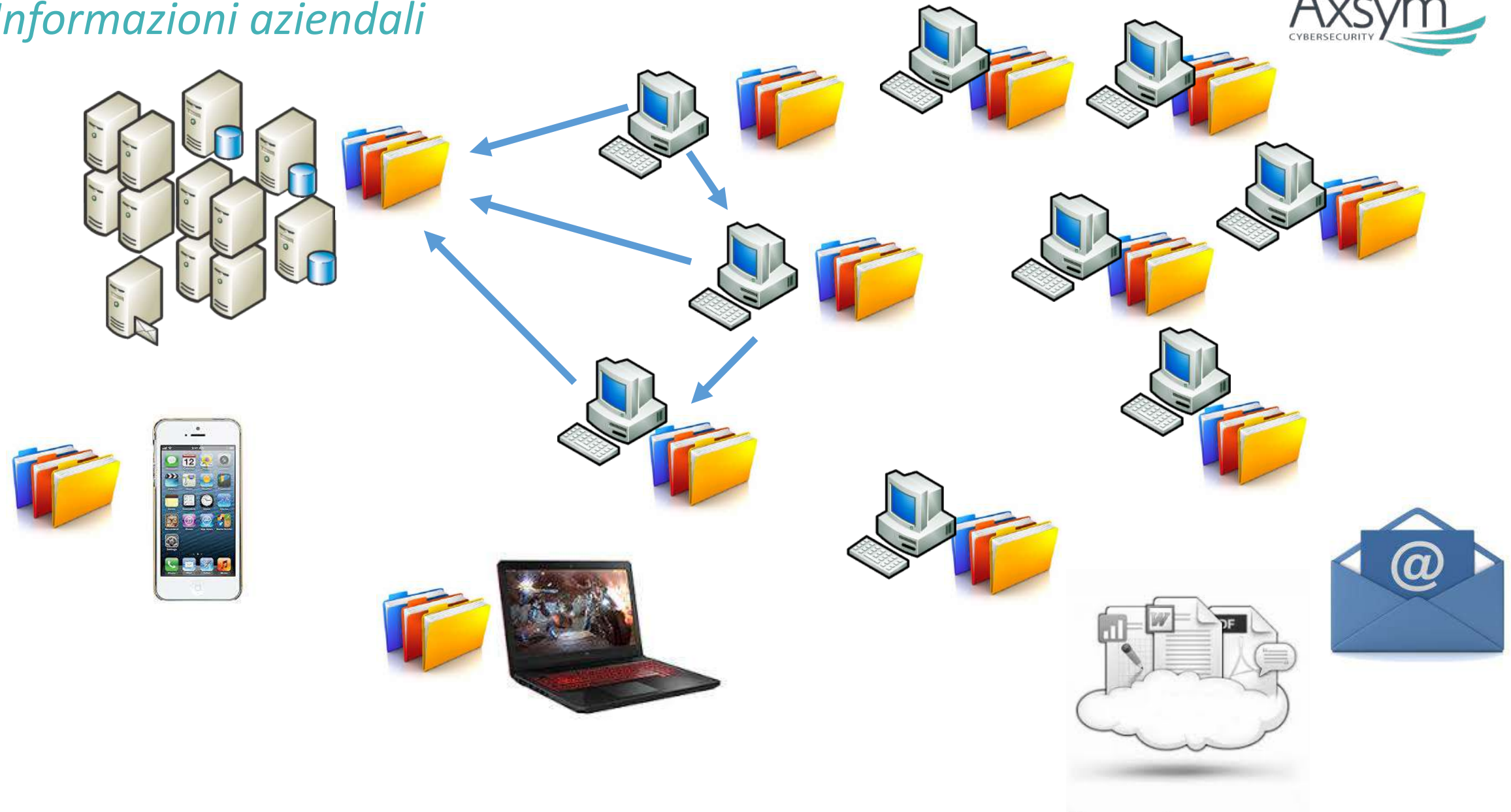
Formazione sull'uso degli applicativi

Gestione del sistema di protezione dati personali

A volte la gestione delle informazioni aziendali viene vissuta come un problema dell'IT

Ma le informazioni sono aziendali, non dell'IT

Informazioni aziendali



Come affrontare il problema?

Informazioni aziendali

Dobbiamo spostare la protezione dal perimetro agli user

Creare consapevolezza negli utenti

Redigere linee guida chiare e trasparenti

Gestire le regole di diffusione delle informazioni

Formazione

Privilegi minimi e gestione password

Monitoraggio

Verificare il grado di sensibilizzazione del personale

Campagne di Phishing Awareness

Tutto questo va inquadrato in una strategia di sicurezza


RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
NIST
CYBERSECURITY
FRAMEWORK

Function del cybersecurity framework

FUNCTION	DESCRIZIONE	OBIETTIVI PRINCIPALI
IDENTIFY	La Function Identify è finalizzata alla comprensione del contesto aziendale.	• Identificazione degli asset che supportano i processi critici di business e dei relativi rischi associati. • Comprensione se risorse e investimenti in Cyber Security sono in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
PROTECT	La Function Protect è associata all'implementazione delle misure di sicurezza necessarie	• Stabilire la protezione dei dati per proteggere la riservatezza, l'integrità e la disponibilità • Gestione della tecnologia di protezione per garantire la sicurezza e la resilienza dei sistemi e dei supporti • Responsabilizzare il personale all'interno dell'organizzazione attraverso la sensibilizzazione e la formazione
DETECT	La Function Detect è associata alla definizione e attuazione di attività appropriate per mantenere il livello di sicurezza implementato e per identificare tempestivamente incidenti di sicurezza informatica.	• Implementazione delle funzionalità di monitoraggio continuo della sicurezza per monitorare gli eventi di sicurezza informatica • Assicurare anomalie ed eventi vengono rilevati e il loro potenziale impatto è compreso • Verifica dell'efficacia delle misure protettive
RESPOND	La Function Respond è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato.	• Garantire la risposta I processi di pianificazione vengono eseguiti durante e dopo un incidente • Gestione delle comunicazioni durante e dopo un evento • Analizzare l'efficacia delle attività di risposta
RECOVER	La funzione Recover identifica le attività appropriate per mantenere i piani di resilienza e ripristinare i servizi compromessi durante gli incidenti di Cyber Security	• Garantire che l'organizzazione implementa processi e procedure di pianificazione del recupero • Implementare miglioramenti basati sulle lezioni apprese • Coordinamento delle comunicazioni durante le attività di recupero

IT Governance

Standard & Law Compliance

Corporate Security Strategy

Audit GDPR

Audit ISO 20000

Business Continuity

Security Incident & Event Management (SIEM)

Disaster Recovery

Security Operations Center (SOC)

Incident & Data Breach Management

Risk Management

Cyber Intelligence

Advisory ISO 20000

Advisory ISO 22301

Advisory ISO 27001

Tra le nostre competenze

WE ♥ TO GET OUR HANDS DIRTY!

La partnership

Axsym CYBERSECURITY

BUSINESS

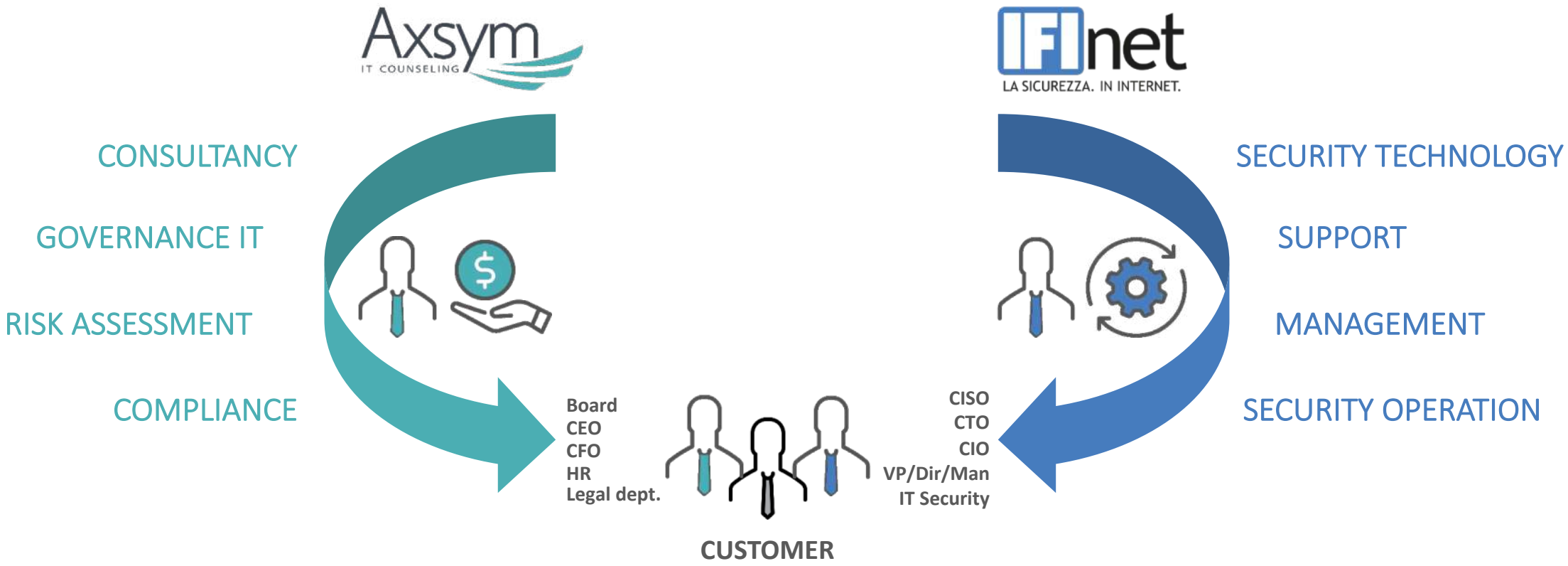
- CONSULTANCY & COMPLIANCE
- GOVERNANCE IT
- RISK & BUSINESS IMPACT ASSESSMENT
- PRIVACY & DPO SERVICES
- TRAINING

IFInet LA SICUREZZA. IN INTERNET.

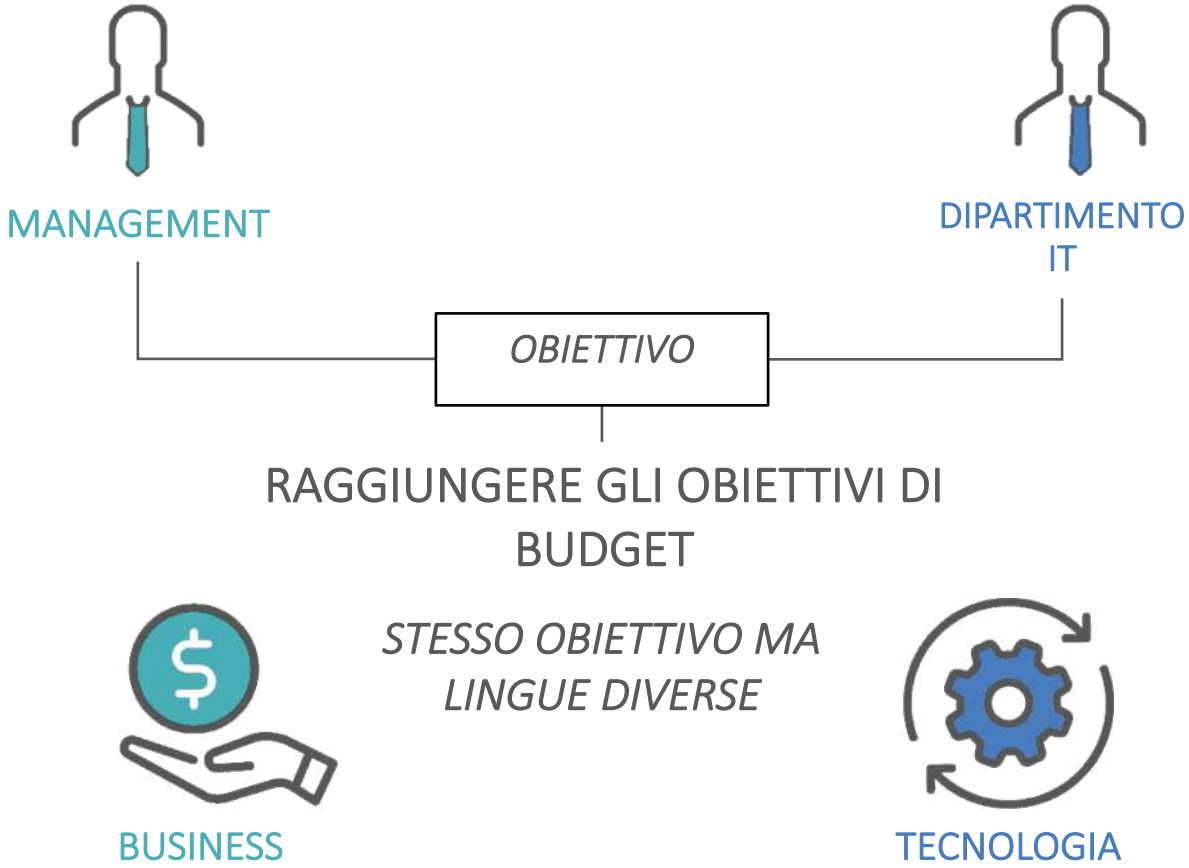
TECNOLOGIA

- DIGITAL TRANSFORMATION
- SYSTEM INTEGRATION
- IT SECURITY
- CLOUD & NETWORKING
- SUPPORT & MAINTENANCE

Cyber consapevolezza



E’ (sempre) un problema di comunicazione



Giovedì 30 maggio – Fumane di Valpolicella (VR)

CLOUD SECURITY *DAY*

CLOUD: NORMATIVA E COMPLIANCE
SICUREZZA PER AMBIENTI SAAS E IAAS
VISIBILITÀ, SICUREZZA E COMPLIANCE DELLE ARCHITETTURE MULTICLOUD
APPLICATION SECURITY, OVUNQUE
CYBERINTELLIGENCE
LA COMPROMISSIONE DEGLI ACCOUNT OFFICE 365

LABORATORIO DEMO E "HANDS ON"

INFO AL DESK IFINET

GRAZIE

AXSYM SRL Corso Porta Nuova, 109 - 37122 Verona, Italia
P.IVA/C.F. 04446280234 Tel. +39 045 5118570 - www.axsym.it - info@axsym.it