CYBERS

PROTECTING YOUR BUSINESS

How to avoid glass breakage

Nikolai Belstein

CEO

CYBERS

“The problem with CISO’s, and the entire cybersecurity field for that matter, is that you keep asking for money and resources but can’t guarantee or even articulate what I am buying”

Un-Named
CFO

Data breaches 2019

Global Averages

Average total cost of a data breach

€ 3,50M

Average size of a data breach

25 575 records

Cost per lost record

€ 137

Time to identify and contain a breach

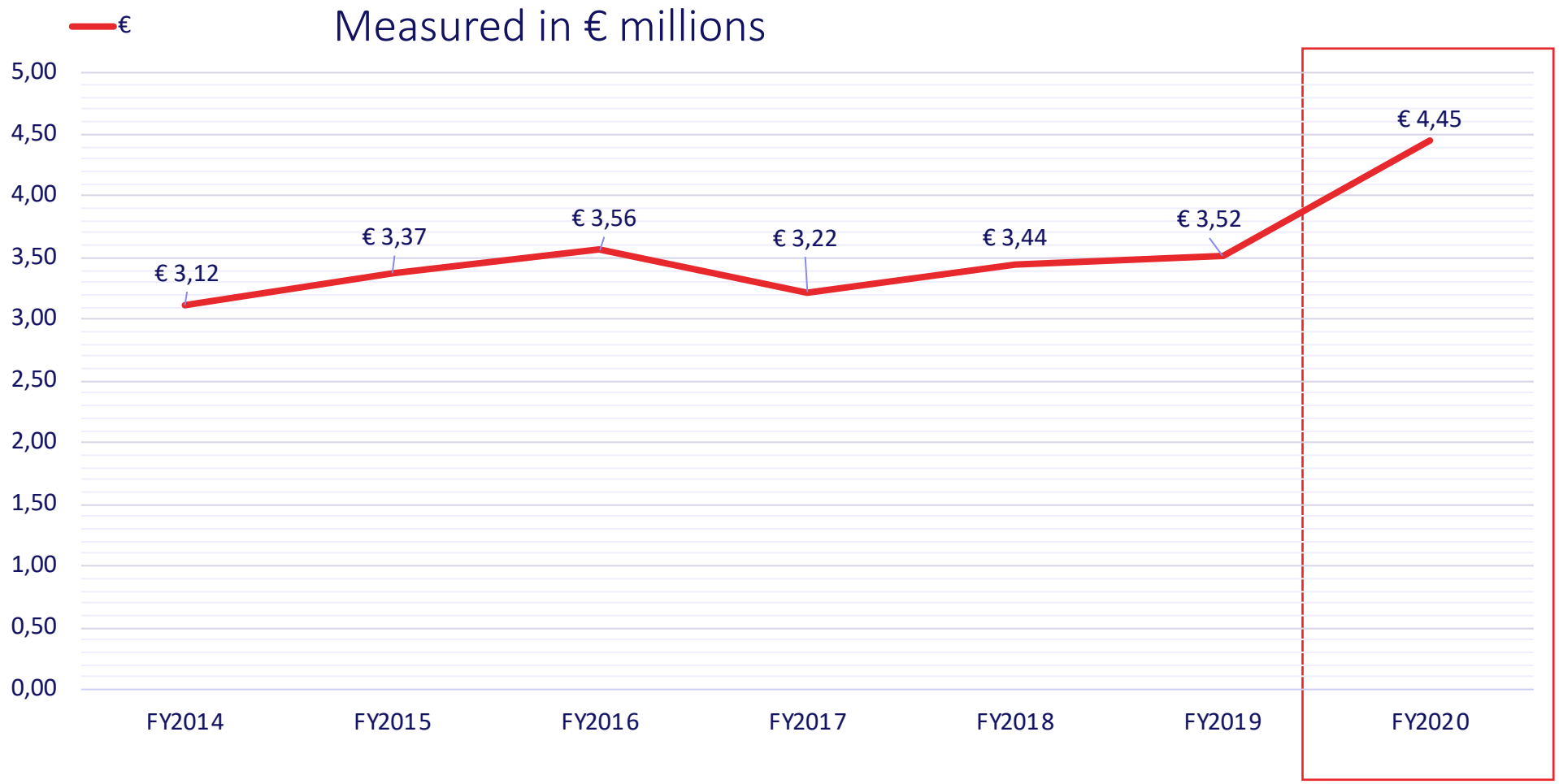
279 Days

Lifecycle of a malicious attack from breach to containment

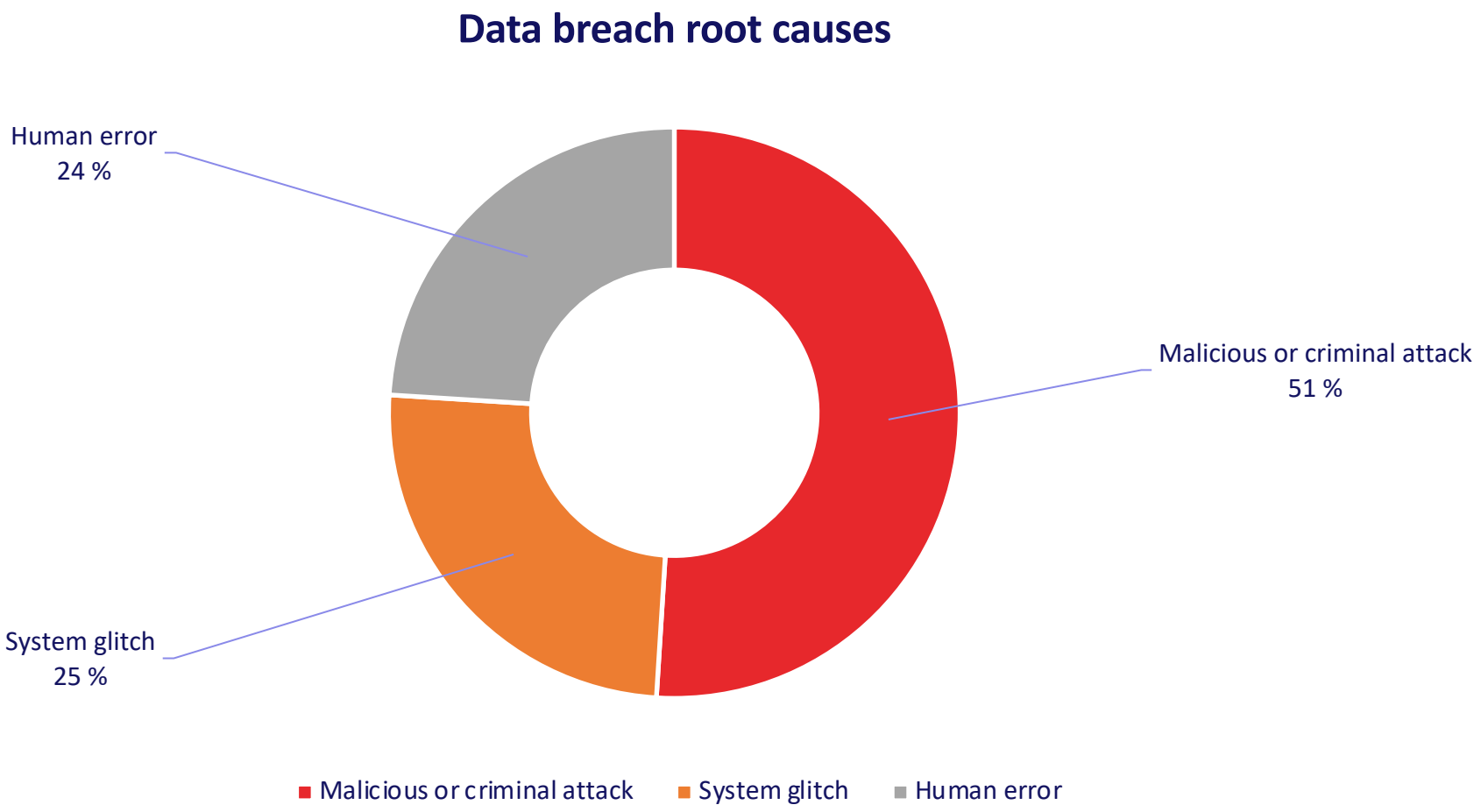
314 Days

Ponemon INSTITUTE

Global average total cost of a data breach



Data breach root causes



CYBERS

Human errors TOP5

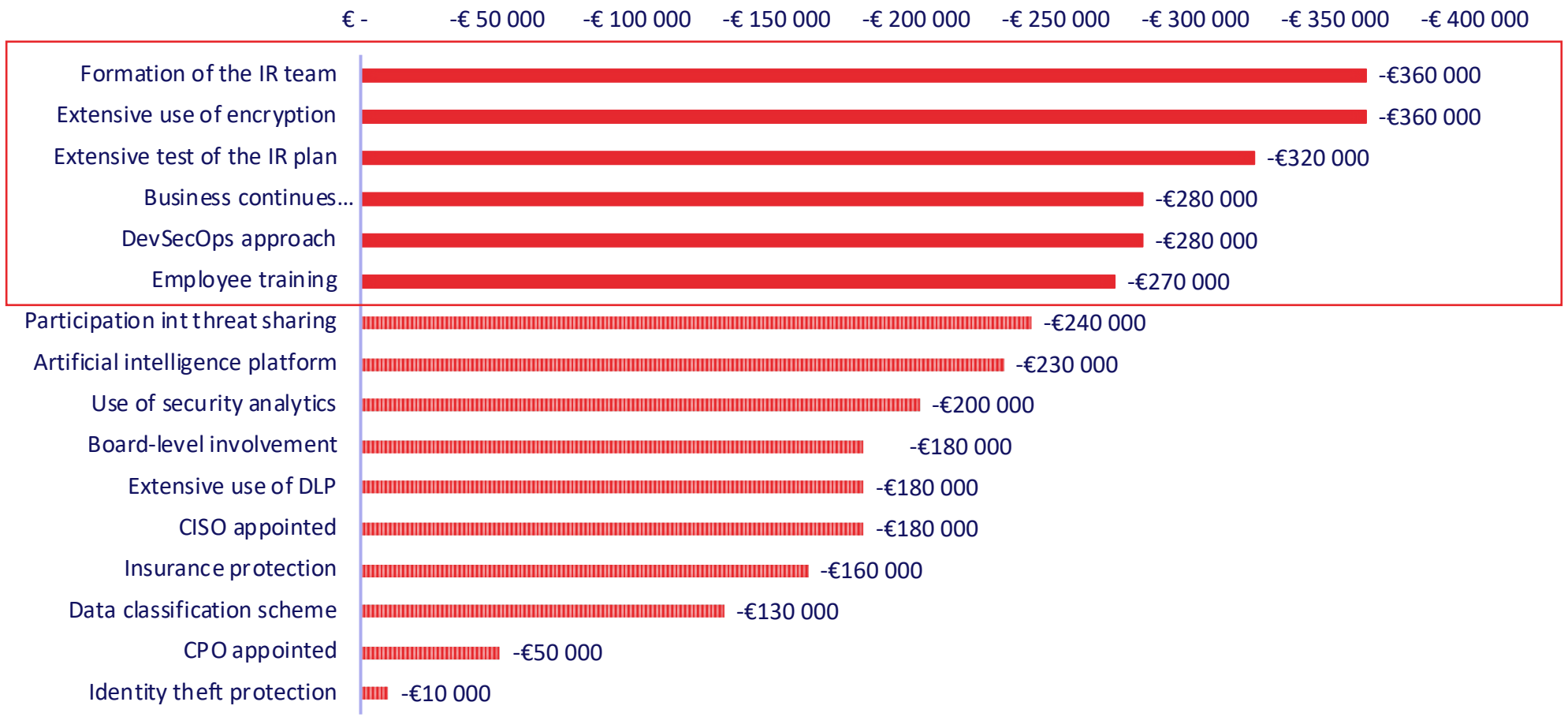
1. Falling for phishing
2. Letting unauthorized users access corporate devices
3. Poor user password practices
4. Poorly managed high privileged accounts
5. Misdelivery

CYBERS

System glitch TOP3

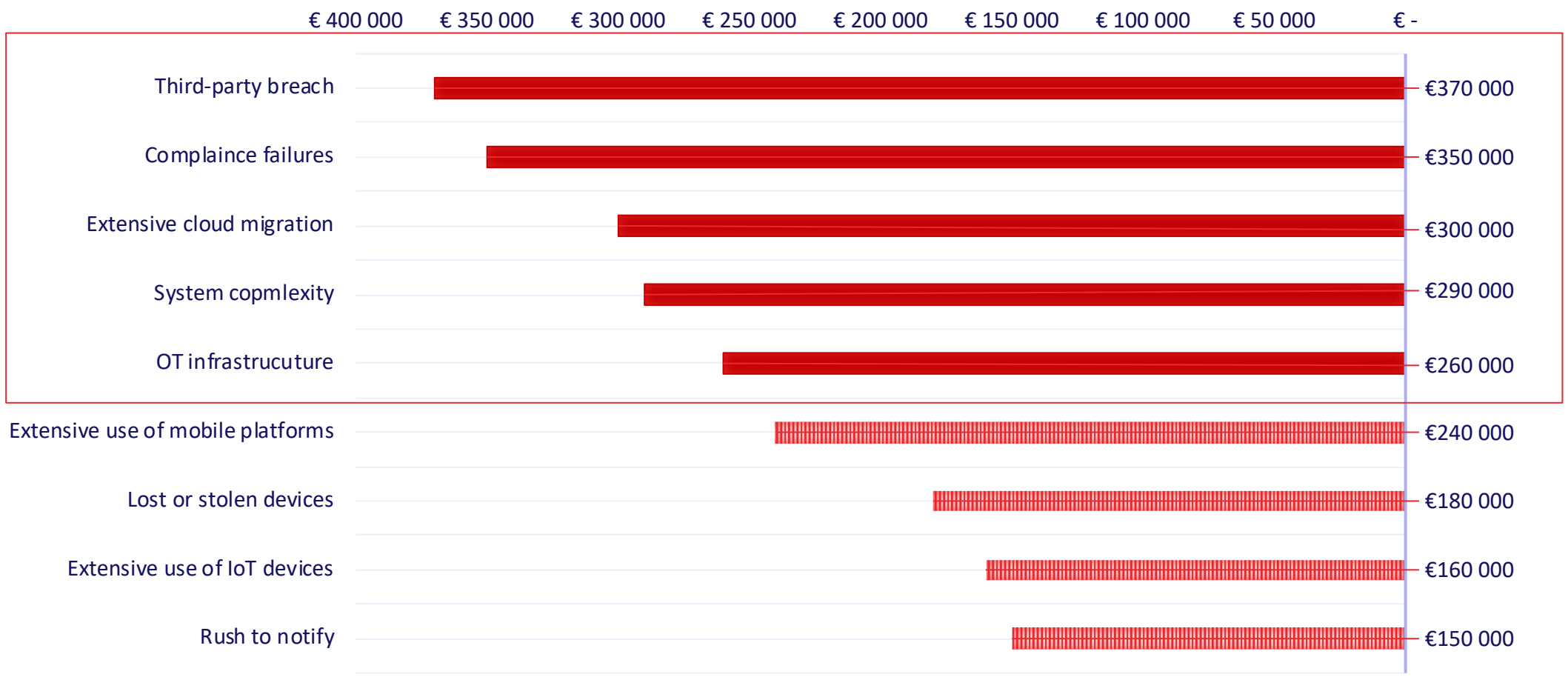
1. Application failures
2. Logic errors in data transfer
3. Inadvertent data dumps

How factors decrease the cost of a date breach



CYBERS

How factors increase the cost of a date breach



The biggest data breach fines

Equifax - $575 Millions

Data breach root course – *poor patching, no vulnerability management, no encryption, missing proper monitoring*

British Airways - $230 million

Data breach root course – *poor 3rd party vendor management, missed penetration testing of their critical application*

Marriott International: $124 million

Data breach root course – *poor overview of their critical assets and NO patching for a legacy infrastructure*

CYBERS

What to do to avoid data breach?

Cyber Hygine rules:

- Cyber security trainings and awareness for all your employees
- Know your risks and risks posture
- Patching and configuration management (inc. Vulnerability management)
- Visibility and monitoring (Security Operation Centre)
    - Have your own Managed Incident Response provider
- Test your backups – restore plan with a real scenarios
- Impement ZERO-TRUST everywhere
- Take a defence in depth as your standard
- Penetration testing before go live for a your critical applications
- Security as a culture everywhere, in all stages and all places in your business
- 3rd party management
- Privilegged access management
- And many more actions

About the CYBERS

- CYBERS is 10 years Cyber Security Boutique
- HQ is in Tallinn, Estonia
- Branch offices
    - Helsinki, Finland
    - Norway, Denmark and Sweden to be open in 2020-21
- 35 FTE’s
- 2019 revenue 3,5M EUR
- Web page: http://cybers.eu

CYBERS

Core Values

The Most:

- Trusted by Customers
- Trusted by Employees
- Reliable for deliveries

CYBERS

Mission

Our mission is to secure your assets and protect your business. We empower customers to respond to cyber threats, innovate their existing security capabilities, and protect their business, by providing world-class cybersecurity services and inspiring our customers to become highly resistant to evolving security threats.

All possible service offerings

CYBERS

Consulting Services	Solutions implementation	Training and education	Managed Security
SOC improvement and development program	Corporate Data Protection: • Network security • Data protection • Endpoint security • Cloud security	Vendor trainings	Security Monitoring: • 24/7 Monitoring • Incident response • Vulnerability management
Security Automation and Systems Integration			
Security Architecture and Design	Threat Detection and Response: • Vulnerability management • Automation & Orchestration • Security event management • Incident response & ticketing • Threat intelligence • Computer forensics • User behavior analytics	• Security awareness trainings • Security technology trainings • DevSecOps and integrations	Security as a Service: • 24/7 monitoring • Policy management • Infrastructure management
Compliance pre-audit services			
Technology security audit			
Security governance development and assessment: • System Security Assessment • Risk Assessment • Security Maturity Assessment • Security Technology Assessment • Compromise Assessment • Security Operations Assessment • Tabletop Exercises	Identity and Access Management: • Privileged Access Management • Public Key Infrastructure • Hardware Security Modules • Multi Factor Authentication		
Penetration testing and Red Team Exercises	Application Security: • Code security assessment • Web & API security • Realtime application security • Penetration testing	Penetration testing and forensics trainings	
Security analytical services			
vCISO – CISO as a Service			

CYBERS

SOCaaS – 8/5 & 24/7/365

CYBERS provides 8/5 and 24/7/365 SOC service for:

- On-prem environment, Hybrid environment, Cloud solutions
- Assured compliance with all industry regulatory rules (HIPAA, PCIDSS and etc)
- Full visibility into event logs, powerful reporting and integration to into your systems
- Easily scalable service that grows as your security needs
- Cloud-based deployment with NO software or hardware cost
- Dashboards for quick identification of potential security and privacy breaches
- Continuous Vulnerability management

CYBERS

CISO as a Service (vCISO)

1. Expertise & Core Competencies
2. Cost Effectiveness
3. Reduced Business Risk & Flexibility to Work on Projects as Needed
4. Improving Your In-House Team
5. Objective Independence

CYBERS

Managed security solutions

- WAF as a Service
- IDPS as a Service
- Endpoint Protection as a Service
- EDR as a Service
- OT and IoT security monitoring
- SIEM as a Service
- Vulnerability management and monitoring
- Secure Web Gateway as a Service
- Secure Email Gateway as a Service

CYBERS

Penetration testing

- Gather valuable insight about the weaknesses and strengths of the system or the application.
- Address vulnerabilities throughout the development lifecycle in a timely fashion.
- Avoid sensitive data leakage and system or application being compromise by cybercriminals.
- Receive a thorough report with a summary of vulnerabilities for executives and managers.
- Receive a detailed report about findings, including remediation guidance and recommendations.

DO'S and DON'Ts NOT to get breached

DO'S

- Use CYBERS services
- On a daily basis behave as you've been breached
- Drive your business based on your cyber risks
- Cyber hygine:
  - Patch management
  - Configuration management
  - Backup
  - Zero-trust
  - SOC / Managed Incident response
  - Use DevSecOps approach
- Follow cyber security best practices

DONT'S

- Don't pay money to a cyber criminals
- Don't think, that you will never get breached
- Don't click on a suspicious URLs and emails
- Don't run your business purely on a compliance needs
- Don't use outdated software
- Don't trust your 3rd party – make a risks assessment
- Don't trust your developers – ensure security

CYBERS

Supported Partners

CYBERS

Thank you