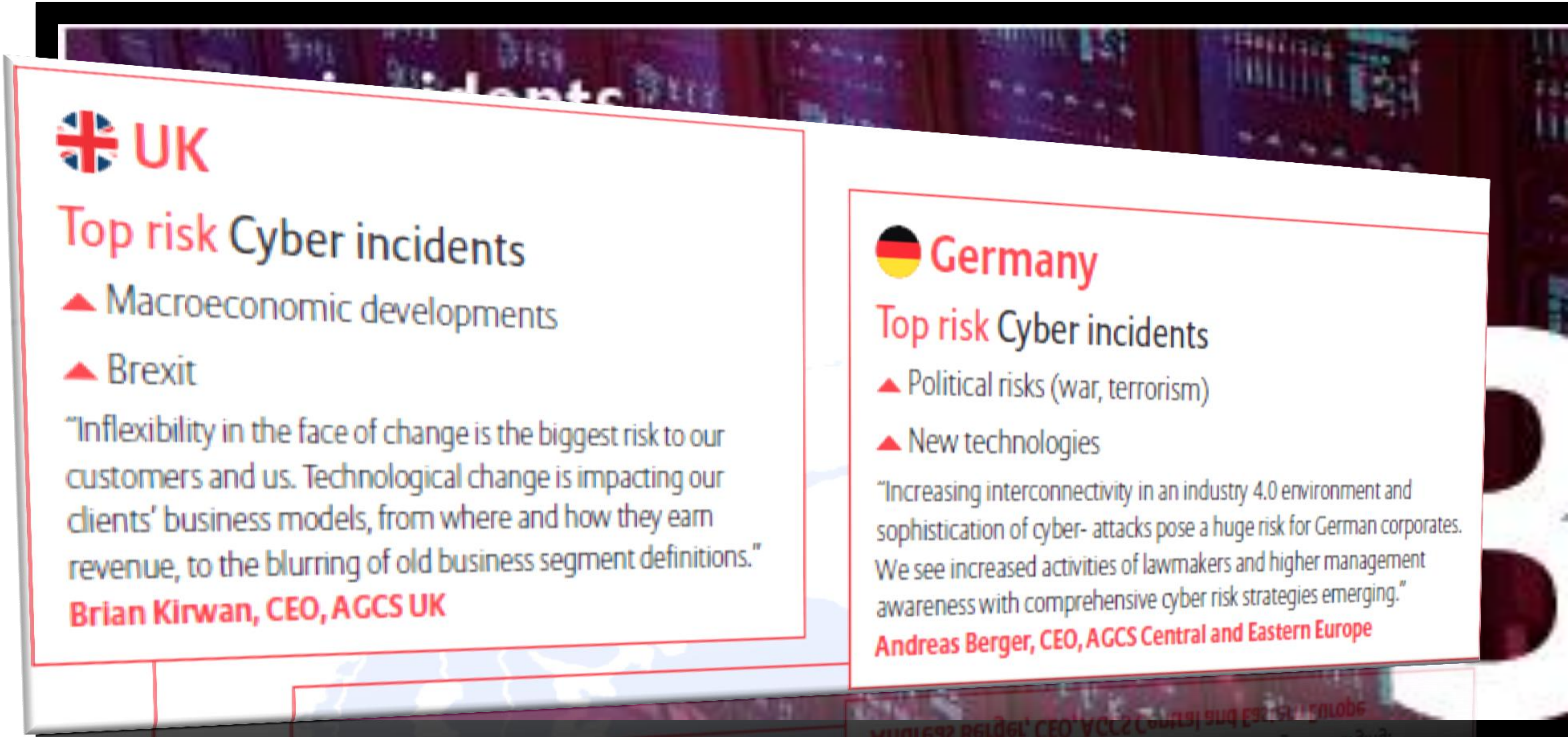
TEACHING PEOPLE THINGS THEY DON’T WANT TO LEARN

Slava Borilin,
Security Awareness Programs Manager



UK

Top risk Cyber incidents

▲ Macroeconomic developments

▲ Brexit

"Inflexibility in the face of change is the biggest risk to our customers and us. Technological change is impacting our clients' business models, from where and how they earn revenue, to the blurring of old business segment definitions."

Brian Kirwan, CEO, AGCS UK

Germany

Top risk Cyber incidents

▲ Political risks (war, terrorism)

▲ New technologies

"Increasing interconnectivity in an industry 4.0 environment and sophistication of cyber- attacks pose a huge risk for German corporates. We see increased activities of lawmakers and higher management awareness with comprehensive cyber risk strategies emerging."

Andreas Berger, CEO, AGCS Central and Eastern Europe

HUMAN MISTAKES AS THE BIGGEST CYBERRISK FOR ENTERPRISES TODAY

over

95%

a percentage of the insider breaches caused by human errors

IBM 2015 Cyber Security Intelligence Index

75%

of the U.K. large organizations suffered staff related security breaches in 2015 (30% more than in 2014)

2015 Information Security Breaches Survey. HM Government in association with InfoSecurity Europe and PwC

50%

of the worst breaches in the U.K. organizations were caused by inadvertent human error

2015 Information Security Breaches Survey. HM Government in association with InfoSecurity Europe and PwC

only

25%

of the cyber insurance plans cover incidents caused by human errors, mistakes and negligence

(while risks caused by external criminals and malicious insiders are covered by 84 and 75% plans respectively)

2015 Global Cyber Impact Report. Ponemon Institute LLC.

MOST SECURITY AWARENESS PROGRAMS – FAILURE REASONS

EMPLOYEE LEVEL

- Time consuming
- Hinders my direct responsibilities
- IT people should do everything, it’s their responsibility
- Who am I to be a target
- IT Security officers are not supportive
- Attacks are rare
- Too difficult
- Too common
- Too technical
- Difficult and abstract
- Easily forgettable
- Not related to business
- You can’t do anything with hackers

- Boring!

CORPORATE LEVEL

- Difficult to manage
- Impossible to train everyone
- Not a priority
- Not supported by C-level
- Non-measurable
- Trainings are passed in a formal way (copying-off)
- Results are not analyzed
- Expensive
- Rarely updated
- Immediate superior requires not to spend time on what does not bring a performance
- Has no connection to reality
- One-time effort (still difficult to manage)

- Non-efficient!

EMPLOYEE LEVEL - DEMOTIVATORS

“Hackers will break my PC”

“I am too small a target”

“I have no time for security”

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

"Smart hackers will send me a virus
and break my PC"

Beware bad people, not broken computers

I understand which criminals can get value from my digital assets and motivated to protect them

"I am too small a target"

"I have no time for security"

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

“Hackers will break my PC”

Beware bad people, not broken computers

Think who can misuse what you do

“I am too small a target”

Small targets are easier and more attractive to cyber criminals

I want to be a harder target than the others

“I have no time for security”

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

“Hackers will break my PC”

Beware bad people, not broken computers

Think who can misuse what you do

“I am too small a target”

You don’t have to be a target to be a victim

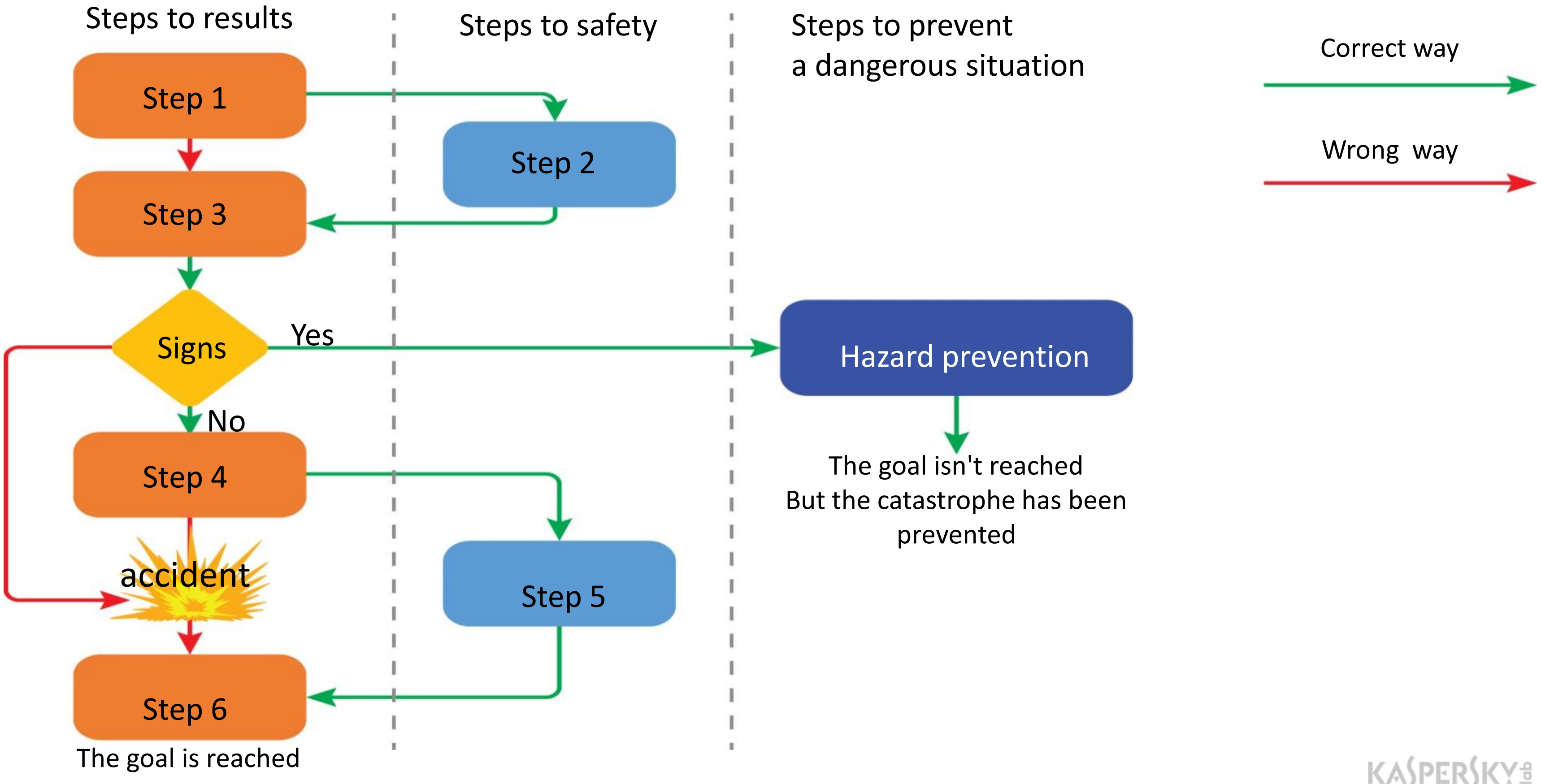
Be a harder target than the others

“I have no time for security”

Security is part of long-term efficiency

I will choose the safest way to achieve the business goal and cooperate with security team

REACH THE GOAL THE SAFEST WAY



TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

"Hackers will break my PC"

Beware bad people, not broken computers

Think who can misuse what you do

"I am too small a target"

You don't have to be a target to be a victim

Be a harder target than the others

"I have no time for security"

Security is part of long-term efficiency

I will choose the safest way to achieve the business goal and cooperate with security team

TRAININGS WITH ORGANIZATIONAL EFFICIENCY

BUILD BEHAVIOR, NOT JUST GIVE KNOWLEDGE

A learning approach should involve gamification, learning-by-doing, group dynamics, simulated attacks, learning paths, etc. It results in strong behavioral patterns and produces a long-lasting cybersecurity effect.

And don’t let your training be boring.

MANAGE PAINLESSLY, MEASURE REAL TIME

Computer-based training programs ensure consistence in training quality as well as flexibility, real-time skills assessment and efficient reinforcement. Automated training assignments, repeated attacks, auto-enrollment in training modules build a long-term efficiency.

Easily managed by Security team or HR/ T&D.

MEET BUSINESS NEEDS AND FORMAT PREFERENCES OF EVERY ORGANIZATIONAL LEVEL

Having different training for different organizational levels and functions creates a collaborative CyberSafety culture, shared by everyone and driven from the top.

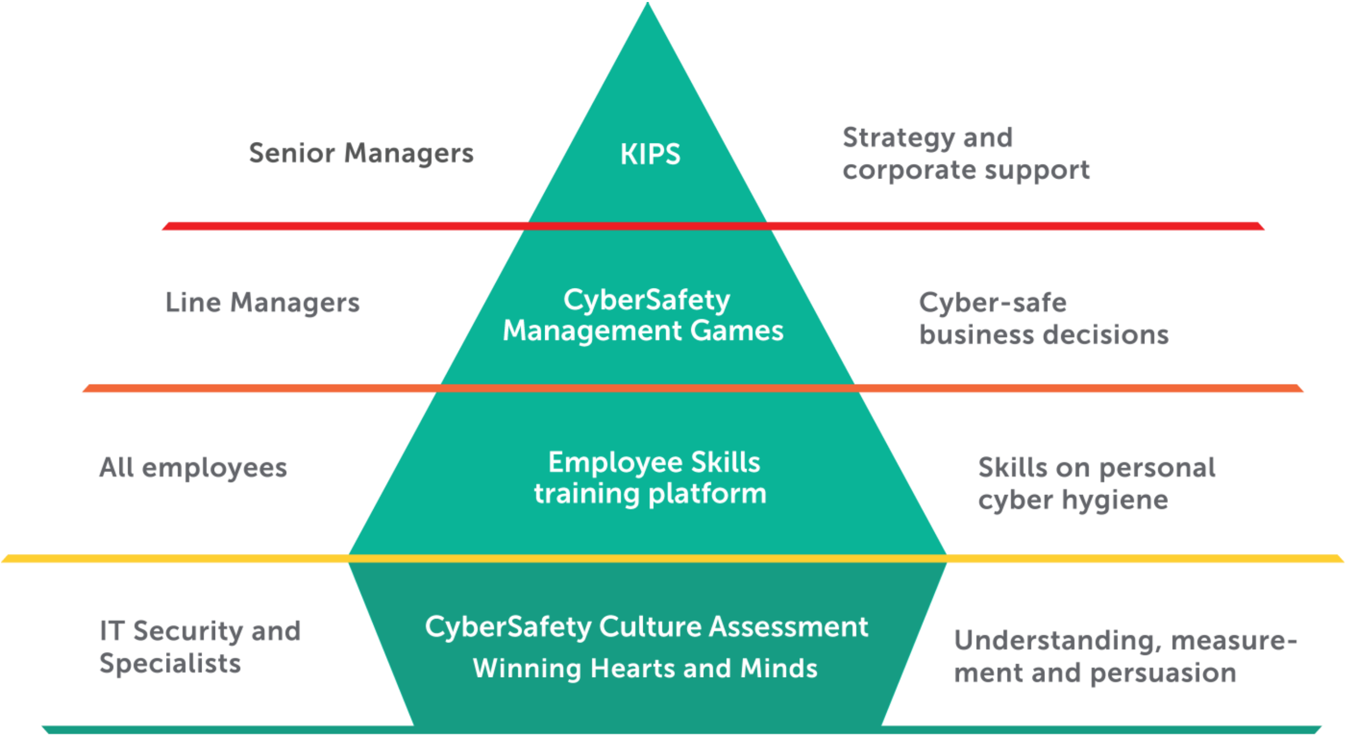
Senior managers, line managers and regular employees need different skills.

BASE EVERY TRAINING ON A STRONG CYBERSECURITY GROUNDS

Don’t think that ‘non-IT’ training does not need a deep cybersecurity expertise. Every training should be based on a strong security model – and be up-to-date towards most recent threats.

That’s how we add to building a safe cyber environment – which is strong, shared and self-sustained.

KASPERSKY SECURITY AWARENESS PRODUCTS



Senior Managers	KIPS	Strategy and corporate support
Line Managers	CyberSafety Management Games	Cyber-safe business decisions
All employees	Employee Skills training platform	Skills on personal cyber hygiene
IT Security and Specialists	CyberSafety Culture Assessment Winning Hearts and Minds	Understanding, measurement and persuasion

1. INTERACTIVE PROTECTION SIMULATION

=> STRATEGIC SUPPORT

For decision makers in Business, IT and Security

KASPERSKY lab
Kaspersky
Interactive Protection Simulation
NETWORK
SHUT DOWN ATM NETWORK
INSTALL AND CONFIGURE ANTI-APT SOLUTION
ATM NETWORK CONTROL SERVER
KASPERSKY lab

- Strategy simulation for decision makers on the cybersecurity
- Team-work
- Competition
- Strategy & mistakes

2 hours PC-based training.
Available as a Train-the-Trainer model.

SCENARIOS	
Corporation	Protecting the enterprise from ransomware, APTs, automation security flaws
Bank	Protecting the financial institutions from high-level emerging APTs
E-Government	Protecting the public web servers from attacks and exploits
Power station / Water Plant	Protecting Industrial control systems

2. CYBERSAFETY MANAGEMENT GAMES

=> DECISION-MAKING SKILLS

For line managers

Understanding

Inner adoption of cybersecurity measures as an important yet uncomplicated time-consuming set of actions

Monitoring

Seeing everyday working process through the cybersafety lens

Cyber-safe decision making

Cybersecurity considerations as an integral part of business processes

Reinforcement and inspiration

Influential leadership and helpful advice to employees

4 hours PC-based training providing managers with competence, knowledge and attitudes essential to maintain secure working environment in their divisions.

Covers all major security domains and typical situations at workplaces.
Available as a Train-the-Trainer model.

KASPERSKY lab

3. EMPLOYEE SKILLS TRAINING PLATFORM

=> CYBER HYGIENE SKILLS

For all employees

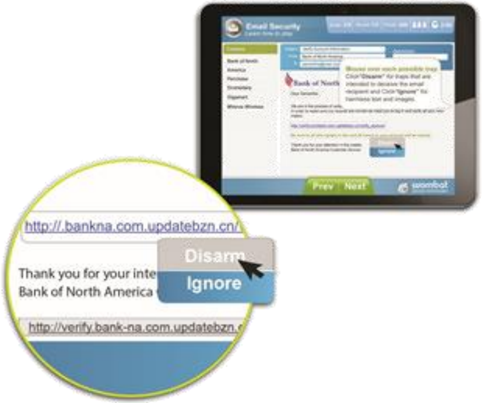
Skills training modules

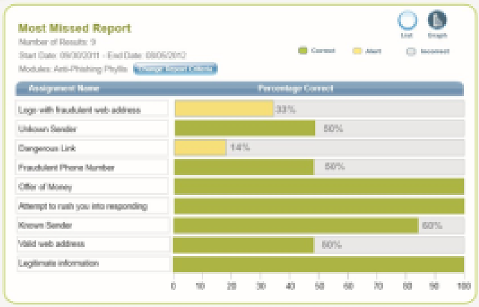
+

Simulated phishing attacks

Knowledge Assessment

Analytics and Reporting





العَرَبِيَّة
čeština
Deutsch
English(UK)
English(US)
español
Español
français
français

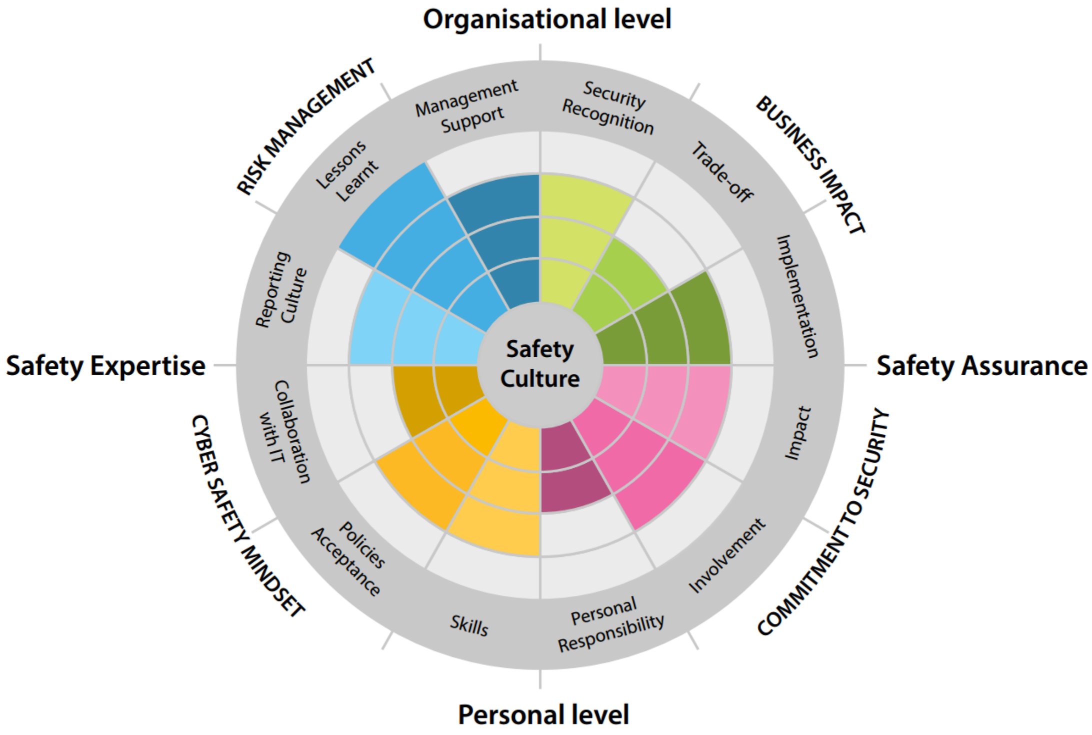
עִבְרִית
Magyar
Íslenska
italiano
日本語
한국어
Nederlands
Norsk
polski

português
русский
Slovák
svenska
ภาษาไทย
Türkçe
tiếng Việt
简体中文
繁體中文

Cloud-based Platform
with multiple administrative roles

4. CYBERSAFETY CULTURE ASSESSMENT

For Chief Information Security Officers



Analyses actual everyday behavior and attitude toward cybersecurity of the all management levels of the enterprise.

Cloud-based survey.
Takes ~15 minutes to complete for an employee.
Consolidated report

CEB SHL Russia&CIS

PROGRAM OUTCOME

up to

90%

A decrease in a total number of incidents

not less than

50%

A decrease in a monetary volume of incidents

up to

93%

Probability of using the knowledge in the daily work

more than

30x

ROI from spending to the security awareness products

amazing

86%

Willingness to recommend the program

RIGHT GOALS, GAMIFICATION AND TAILORED SET OF TRAININGS

EXAMPLES

TOTAL

Telefonica

nutreco

Eneco

Kcell

AGIPI

econocom

Bonfiglioli
Forever Forward

HIDROMEK

Eurasian Bank

QIB المصرف

SBERBANK
By your side

HOME
CREDIT
BANK

LKQ

Senato
della Repubblica

BUNDESKANZLERAMT ÖSTERREICH

ESPACE
HABITAT

Gobierno
de la Rioja

air astana

WE PROTECT WHAT MATTERS MOST

KASPERSKY lab