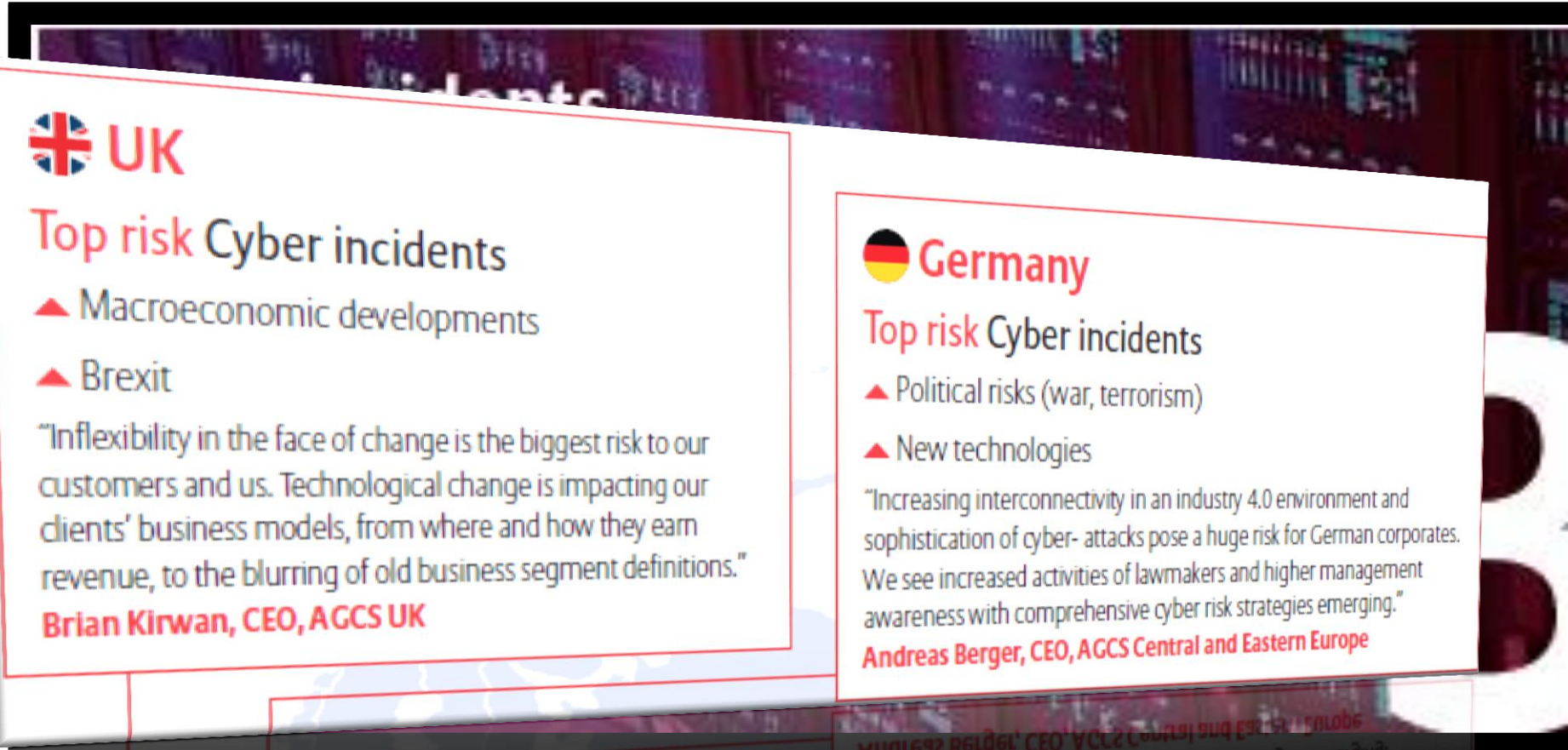
TEACHING PEOPLE THINGS THEY DON'T WANT TO LEARN

Теплова Ольга,
Security Awareness Programs Manager

KASPERSKY lab



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

ИНОФРМАЦИОННАЯ БЕЗОПАНОСТЬ – ЭТО ЛЮДИ

80% всех инцидентов начинаются с ошибки обычного сотрудника

Сотрудники сами

- Игнорируют опасности
- Устанавливают вирусы
- Выдают конфиденциальные данные
- Нарушают правила ИБ

Наиболее уязвимые места: HR, PR, секретариат, поставщики

KASPERSKY

ВЛИНИЕ КИБЕР-ИНЦИДЕНТОВ

- Котировки и капитализация
- Конкурентоспособность
- Активы
- Регулирование и штрафы
- Карьера менеджеров
- Административная и уголовная ответственность

ПОЧЕМУ ВОЗНИКАЕТ НЕДОВОЛЬСТВО ОБУЧЕНИЕМ

ДЛЯ СОТРУДНИКА

- Требует много времени
- Мешает исполнению моих обязанностей
- Это ответственность ИТ подразделений
- Я не являюсь целью мошенников
- ИБ не оказывает поддержки
- Атаки происходят редко
- Это слишком сложно
- Это исключительно технические знаний и навыки
- Сложно и абстрактно
- Быстро забудется
- Не нужно для бизнеса
- Я ничего не могу сделать с хакерами

- Скучно!

ДЛЯ ОРГАНИЗАЦИИ

- Сложно управлять
- Невозможно научить каждого
- Не является приоритетным
- Не поддерживается руководителями
- Не измеримо
- Формализм при обучении
- Результаты сложно проанализировать
- Дорого
- Не надо тратить время на то, что не влияет на производительность
- Не имеет отношения к реальности
- Одноразовый эффект

- Не эффективно!

ДЕМОТИВИРУЮЩИЕ УСТАНОВКИ

“Умные хакеры сломают мой компьютер”

“Я не представляю интереса для кибер-преступников”

“У меня нет времени на безопасность”

СМЕНА УДЕЖДЕНИЙ

“Умные хакеры сломают мой компьютер”

Опасайтесь людей, а не сломанных компьютеров

Подумайте, кто может легко воспользоваться тем, что вы делаете

“Я не представляю интереса для кибер-преступников”

“У меня нет времени на безопасность”

СМЕНА УБЕЖДЕНИЙ

“Умные хакеры сломают мой компьютер”

Опасайтесь людей, а не сломанных компьютеров

Подумайте, кто может легко воспользоваться тем, что вы делаете

“Я не представляю интереса для кибер-преступников”

Страдают не крупные, а доступные мишени

Станьте менее уязвимым, чем другие

“У меня нет времени на безопасность”

СМЕНА УБЕЖДЕНИЙ

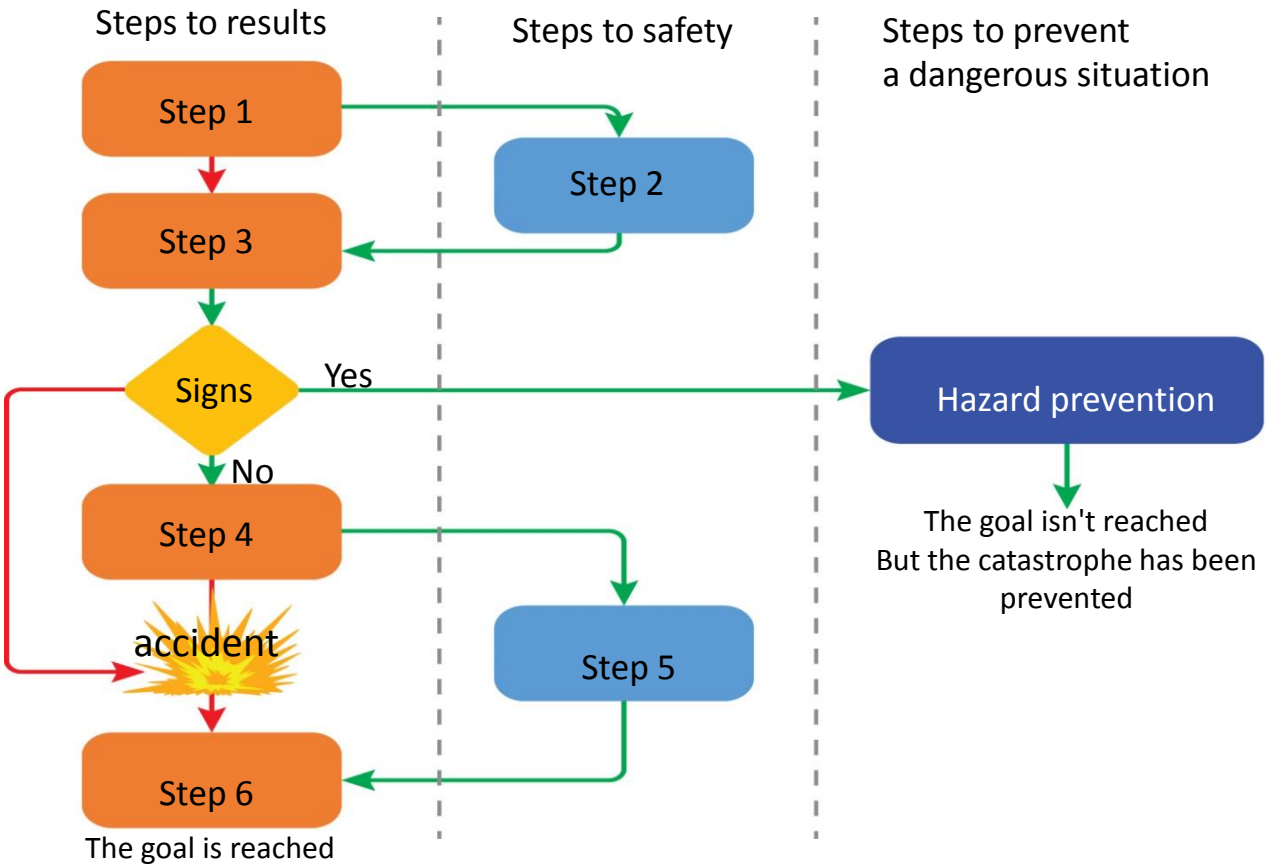
“Умные хакеры сломают мой компьютер”	“Я не представляю интереса для кибер-преступников”
Опасайтесь людей, а не сломанных компьютеров	Страдают не крупные, а доступные мишени
Подумайте, кто может легко воспользоваться тем, что вы делаете	Станьте менее уязвимым, чем другие

“У меня нет времени на безопасность”

Безопасность необходима для эффективной работы

Сотрудничайте, а не торгуйтесь, с отделом ИБ

REACH THE GOAL THE SAFEST WAY



Correct way

Wrong way

ПРОГРАММА РАЗВИТИЯ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ ЛАБОРАТОРИИ КАСПЕРСКОГО

Структура тренингов «Лаборатории Касперского» по повышению осведомленности в области кибербезопасности

KIPS (СТРАТЕГИЯ)

Формат

Интерактивная онлайн бизнес-симуляция, группы от 10 до 500 человек, 2 часа
Возможно проведение как в онлайн-формате, так и в формате очного тренинга.

Для топ-менеджеров и руководителей отделов IT и ИБ

Цели и задачи бизнес-симуляции

1. Понимание степени влияния информационной и кибербезопасности на устойчивое развитие компании
2. Изучение современных угроз и типовых ошибок, совершаемых при построении политики ИБ
3. Отработка взаимодействия между подразделениями и отделом ИБ для обеспечения устойчивости к киберугрозам

Возможные вариации сценария	
Корпорация	Защита торговых и промышленных компаний от ransomware, целевых атак и прочих уязвимостей
Банк	Защита финансовых институтов от вновь возникающих целевых кибератак высокого уровня
Электронное правительство	Защита публичных электронных сервисов от атак и эксплойтов
Электростанция	Защита промышленных компаний и объектов инфраструктуры (на примере газотурбинной электростанции)

МЕНЕДЖЕРСКИЕ НАВЫКИ CYBERSAFETY MANAGEMENT GAMES (УПРАВЛЕНИЕ)

Для линейных руководителей и руководителей среднего звена

Цели и задачи бизнес-симуляции

1. Понимание и анализ ИБ рисков подразделения
2. Формирование навыка анализа и контроля соблюдения правил ИБ подчиненными
3. Формирование мотивации и умения принимать бизнес-решения с учетом принципов ИБ

Формат

Интерактивная он-лайн бизнес-симуляция, группы от 10 до 50 человек, 4 часа

ПЕРСОНАЛЬНЫЕ НАВЫКИ (ОБУЧЕНИЕ НАВЫКАМ)

Для всех сотрудников

Обучающие модули

+

- Симулированные фишинг-атаки
- Оценка знаний
- Аналитика и отчетность

Облачная платформа с большим выбором административных ролей

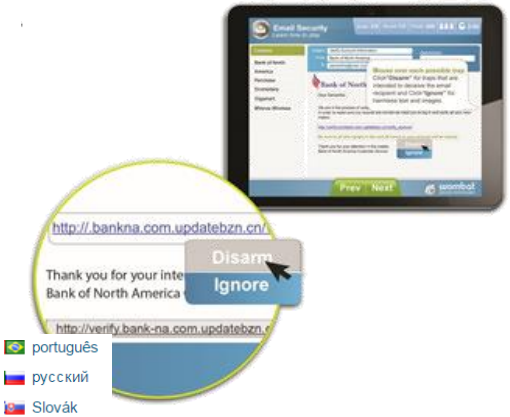
Цели и задачи

Получение знаний и отработка персональных навыков, необходимых для соблюдения ИБ в ежедневной работе

Формат

Набор дистанционных модулей, 10 модулей, 1 модуль – 20 минут

العَرَبِية
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
tiếng Việt
简体中文
繁體中文



KASPERSKY

SECURITY AWARENESS PROGRAMS CAN TURN CYBER SECURITY INTO A POSITIVE MODEL

KASPERSKY lab

SECURITY AWARENESS = FACE AND VOICE OF SECURITY DEPT.

A Word to CISOs Seeking to Purchase Security Awareness CBTs

CISOs and other purchasers of security awareness CBT products should resist basing their vendor evaluations solely on technical/functional requirements. Deployment of security awareness materials — in many ways — becomes the overt face and voice of the security department to the rest of the organization. As such, ensuring that the tone, production value, and overall look and feel of the solution are a good match for your specific organization is fundamental to success.

Magic Quadrant for Security Awareness Computer-Based Training

Published: 25 October 2016 **ID:** G00293102

Analyst(s): *Perry Carpenter* | *Joanna G. Huisman*

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.

EXAMPLES


TOTAL


du
add life to life


ITW


AGIPI


ict
QATAR


ISA


Telefónica


Barilla


QIB
المصرف


Senato
della Repubblica


CERN


nutreco


econocom


بنك الدوحة
DOHA BANK


Gobierno
de la Rioja


GORI


Eneco


ROSATOM

RusHydro


DOLPHIN
ENERGY
دولفين
للطاقة


SBERBANK
By your side


YOKOGAWA


ENTE d'AMBITO
SARNESE VESUVIANO


BASF
We create chemistry

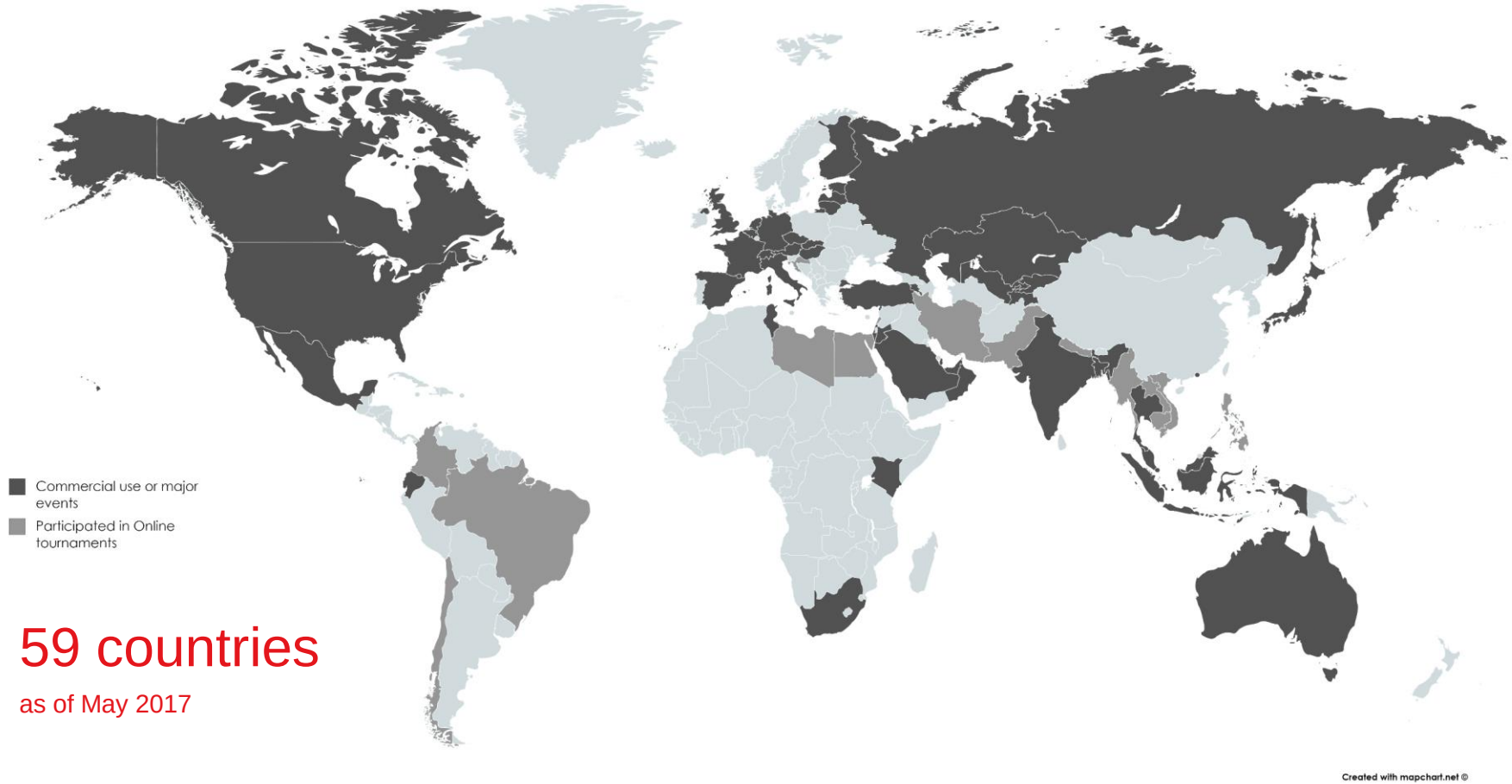

LKQ


TOSHIBA


Eurasian Bank

BUNDESKANZLERAMT ÖSTERREICH

KASPERSKY SECURITY AWARENESS INITIATIVES WORLDWIDE



59 countries

as of May 2017

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


WE PROTECT WHAT MATTERS MOST
KASPERSKY lab