KASPERSKY lab

CYBERSAFETY CULTURE ASSESSMENT

CyberSafety Culture Assessment[1] analyses actual everyday behavior and attitude toward the cybersecurity at all levels of the enterprise, showing how employees in your organization perceive different aspects of cybersecurity.

Assessment results can be used to understand the misbalances and areas to focus on, to justify and align priorities in the internal and external activities of the Security department, including awareness and trainings, internal PR and information sharing, collaboration principles while working with business.

CyberSafety Culture includes domains, which will be assessed and measured altogether, organization-wide. The assessment results are the basis for discussion of the role and place of cybersecurity in supporting the business efficiencies:

- CyberSafety Mindset (perception of security & policies),
- Risk Management (guidance, feedback, improvements),
- Commitment (people's attitude and behavior on security),
- Business Impact (the balances between security and business efficiency).

Focus

Assessment looks at security culture from different perspectives:

- Organizational (managerial) level
- Personal (Employee) level
- Expertise available
- Security Assurance as a process

PLEASE NOTE THAT CYBERSAFETY CULTURE REPORT IS NOT AN ASSESSMENT OF THE TECHNICAL SECURITY MATURITY LEVEL OF THE ENTERPRISE, NOR IS IT A MEASUREMENT EFFECTIVENESS OF THE SECURITY DEPARTMENT.

The CyberSafety Culture report shows how average employees see / feel cybersecurity in their minds; what do they think about the culture, habits, rituals, daily practice for cybersecurity related aspects; what is their personal perception of different aspects of the culture of making the company secured from the cyber threats. Such perception results from various company practices and units, not just a result of security or risk management department activity.

The Assessment is performed as a cloud-based survey. It takes about 15 minutes to complete for an employee, average 2 weeks to run the survey though all employees.

After the survey the customer receives a consolidated report.

[1] CyberSafety Culture Assessment is a collaborative study made by Kaspersky Lab & CEB/SHL. © 2015-2017

Below is the description of the diagnosis model used in CyberSafety Culture Assessment.

CyberSafety Mindset	
Collaboration with IT (Security team)	Employees of non-IT departments see IT (Security) staff as allies, partners and friends: they are encouraged to ask for help and receive it timely and in full, when they do
Policies Acceptance	Employees accept safety regulations and policies as reasonable and not overly restrictive
Skills	To assure that employees know how to act when they face a CyberSafety hazard and how to identify one, they are properly trained and kept up-to-date

Risk Management	
Management Support	Line managers/ supervisors actively support and promote CyberSafety among their subordinates; they make sure employees act cybersafely
Lessons Learnt	Reported safety concerns are quickly analyzed and employees are given instructions on how to act if a similar situation occurs in the future
Reporting Culture	See Something – Say Something: CyberSafety incidents are timely reported; employees know they can report such incidents without being punished in any way

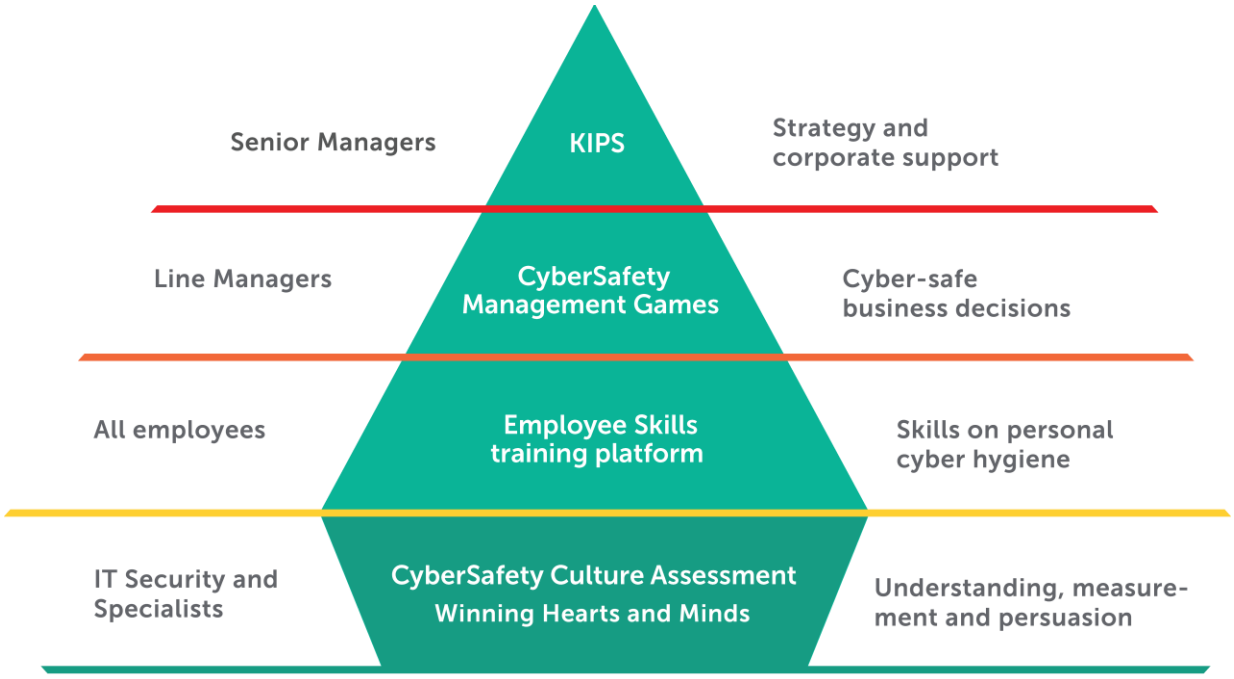
Business Impact	
Implementation	Changes in Cyber Safety policies and regulations are implemented with regard to employees' expectations; the need for such changes is explained to them in detail
Trade-off	Whenever a conflict of interest between security requirements and business needs arises, a compromise is reached: business goals are met without compromising security
Security Recognition	Company management recognizes the necessity to assure CyberSafety and see it as an essential part of business continuity

Commitment to Security	
Involvement	Employees take extra effort and voice their concerns regarding CyberSafety even when it is not their direct responsibility
Personal Responsibility	Employees understand that not only IT/ Information Security department is responsible for CyberSafety assurance; thus, they take responsibility for acting cyber safely
Impact – my actions matter	Employees understand how their actions and decisions affect the "bigger security picture": they see the connection between their everyday work and CyberSafety

Kaspersky Security Awareness Training Products

CyberSafety Culture Assessment is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology. CyberSafety Culture is a set of values and attitudes that drives people's behavior, on an individual or corporate level.

We help customers develop a CyberSafety Culture, under the management of their security and HR teams, through a set of awareness training programs. The training programs utilize gamification and address all levels in the organization structure.



COMPREHENSIVE BUT SIMPLE AND STRAIGHTFORWARD

- Wide range of security issues
- Familiar environments
- Engaging training process
- Practical exercises
- Language suitable for non-IT people

BUSINESS BENEFITS

- As much as 93% probability of using the knowledge in the daily work
- Decrease the number of incidents by up to 90%
- Reduce the cyber risk monetary volume by 50-60%
- Translate the cybersecurity from IT-jargon to business language, and get business management involvement
- Get measurable cybersecurity awareness program results
- Provide ROI from investment into the Security Awareness more than 30x times