KASPERSKY lab

Cybersafety Culture Assessment

Target-based learning program: culture & attitudes

kaspersky.com/awareness
#truecybersecurity

Cybersafety Culture Assessment

Focus

Assessment looks at security culture from different perspectives:

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

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).

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

Cybersafety Culture report structure

- Current state of Cybersafety Culture by each aspect in your organization
- Break down of the results by different company's locations, organizational levels, positions and demographical groups
- Company's results in comparison with global data

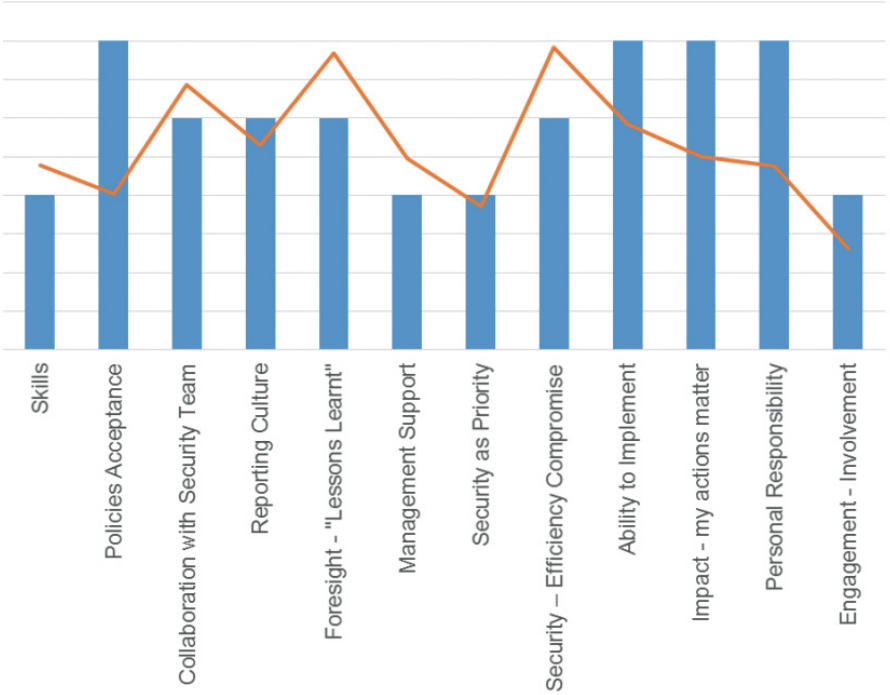
Global Cybersafety Culture research data for benchmarking

In 2017 Kaspersky Lab together with IDC conducted a global Cybersafety Culture research, which provided data on attitudes employees of large organizations (500+) have towards cybersecurity.

Kaspersky Lab provide this data in order to evaluate company's results in comparison with global average data for determining on which aspects of cybersecurity should focus more and for better targeting in setting goals and objectives for cybersecurity activities.

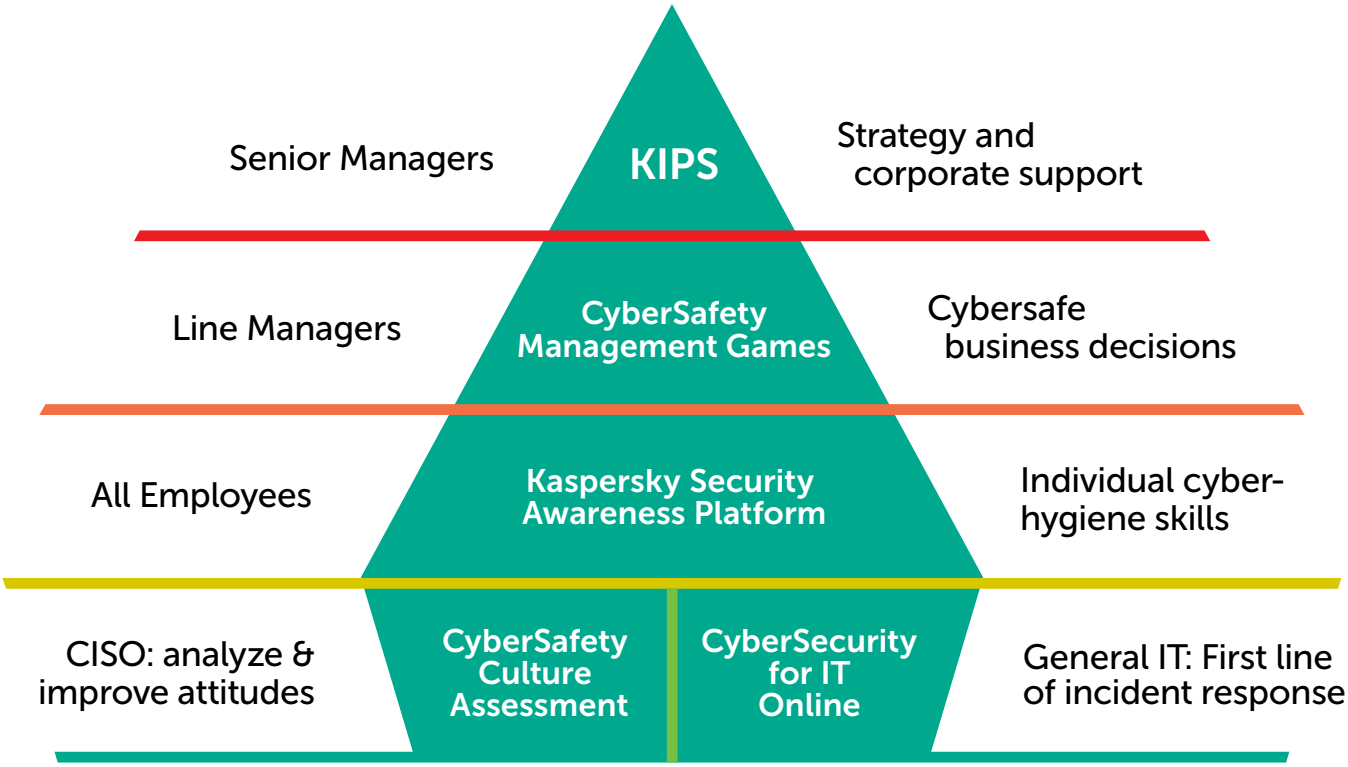
Here is an example of how it looks like in the report:

Results of the Company (blue) vs World average (red)



Kaspersky® Security Awareness

Kaspersky Lab has launched a family of computer-based gamified training products that utilize modern learning techniques and address all levels of organizational structure. This approach helps create a collaborative cybersafety culture which engenders a self-sustaining level of cybersecurity throughout the organization.



Setting objectives & choosing a program

Setting goals based on global data

Benchmarking against world/ industry averages

Learning management

Learning automation

Self-adjusting learning path

Calculation on time spent

Reporting & analytics

Actionable reports anytime

On-the-fly analysis of potential for improvement

Program efficiency & appreciation

True gamification

Competition & challenge

Overload prevention

up to
90%
Reduction in the total number of incidents

not less than
50%
Reduction in the financial impact of incidents

up to
93%
Probability that knowledge will be applied in everyday work

more than
30x
ROI from investment in security awareness

amazing
86%
Of participants willing to recommend the experience

www.kaspersky.com

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Kaspersky Security Awareness: **www.kaspersky.com/awareness**
Product demo: **www.kaspersky.com/demo-sa**