Kurk Lietuvai

LITHUANIAN SMALL AND MEDIUM ENTERPRISES (SME) CYBER SECURITY SURVEY

Administered by the “Create Lithuania” team at the Ministry of National Defense, this survey aims to assess the awareness levels of cyber security threats from Small and Medium Enterprises (SME) and understand the top cyber security issues they typically face The survey of SMEs' CEOs and employees was conducted via the "e.citizen" ("*e.pilietis*") platform in November and December 2019. A total of 227 respondents participated in this assessment.

129 SME CEOS

129 SME CEOs took part in this survey to answer questions about the level of cyber security vulnerability and awareness in their company.

COMPANY SIZE

41% of respondents were from micro enterprises (up to 10 employees), 40% were from small enterprises (between 10-50 employees), and 19% were from medium enterprises (between 50- 250 employees).

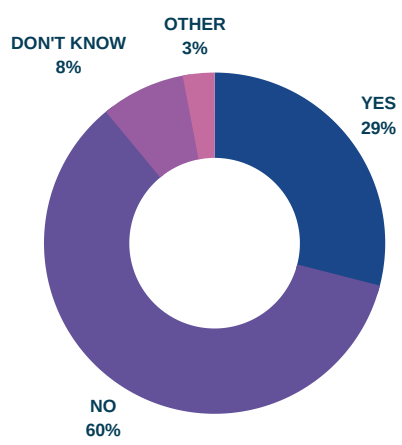
COUNTIES

The survey involved respondents from all 10 counties in Lithuania. The highest number of CEOs came from Vilnius (25%), Utena (17%) and Šiauliai (9%) counties.

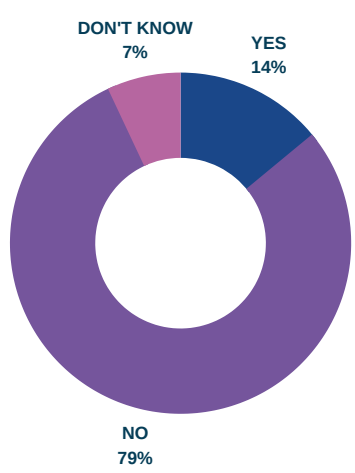
AREA OF ACTIVITY

The highest amount of respondents came from wholesale and retail trade (21%), construction (16%), and administrative and support services (12%).

Does your organisation have a formal policy or documentation outlining cyber security processes and risks within your company?



Have you carried out a cyber security risk assessment within your assessment in the last 12 months?



72 % of SMEs said they do not know or are not sure if they can assess and evaluate cyber security risks and gaps.

74%
ARE NOT READY OR DO NOT KNOW IF THEY ARE READY TO WITHSTAND A CYBER ATTACK.

44%
DO NOT BELIEVE OR ARE NOT SURE THAT THEY COULD BE A VICTIM OF A TARGETED ATTACK.

58%
AGREE THAT A CYBER INCIDENT WOULD HAVE A SIGNIFICANT IMPACT ON THEIR COMPANY.

Companies with an implemented cyber security policy claim to feel more prepared (43%) to withstand a cyber attack than those with no such policy (18%).

1 out of 2 SMEs received fraudulent emails (*phishing*) in the last 12 months.

1 out of 5 CEOs responded that they do not know what cyber incident(s) may have occurred in their company in the last 12 months.

More than half of SMEs who claimed to have experienced a cyber breach said they do not know what were the consequences and the financial cost of attacks.

26% ORGANIZED CYBER SECURITY TRAINING FOR THEIR EMPLOYEES.

57% SAID THEY DO NOT HAVE ENOUGH SUFFICIENT AND NECESSARY KNOWLEDGE TO CHOOSE CYBER SECURITY MEASURES.

€0 **40 % of SMEs** have not invested a single euro into their company's cyber security measures in the last 12 months.

76 % AGREED THAT IT IS IMPORTANT THAT THEIR BUSINESS PARTNERS MEET AND COMPLY WITH CYBER SECURITY STANDARDS.

37 % AGREE THAT A CYBER SECURITY ASSESSMENT CERTIFICATE WOULD BENEFIT THEIR COMPANY.

SME EMPLOYEES SURVEY (98 RESPONDENTS)

TRAININGS
82%
DID NOT PARTICIPATE IN CYBER SECURITY TRAINING IN THE LAST 12 MONTHS.

EMPLOYEES
86%
AGREE THAT ALL EMPLOYEES ARE IMPORTANT TO ENSURE THEIR COMPANY'S CYBER SECURITY.

INFORMATION
14%
AGREE THAT THERE IS ENOUGH EASILY ACCESSIBLE AND UNDERSTANDABLE INFORMATION ABOUT CYBER SECURITY.

ABOUT THE PROJECT

gabriele.bileviciute@kurklt.lt justas.kidykas@kurklt.lt ruta.beinoriute@kurklt.lt