HOW DO COMPANIES MAKE A SHIFT TO REMOTE WORK?

HAVE YOU MOVED YOUR EMPLOYEES TO WORK REMOTELY?

57,1%

Only those who can work remotely

42,9%

Yes, 100% of employees were moved to work remotely

3,6%

Couldn't move employees to work remotely

1,8%

Haven't moved as it seems impractical

DO YOU CONTROL YOUR REMOTE EMPLOYEES?

39,3%

Yes, we do, we make calls during work hours, require them to write reports

10,7%

Control discipline with the help of time tracking software

16,1%

Control employees and data transfer with the help of DLP systems

42,9%

No, we don't

THE NUMBER OF INTERNAL INCIDENTS … AFTER THE COMPANY WENT REMOTE

32,1%

…remained the same…

17,9%

…decreased…

10,7%

…increased…

39,3%

I don't know

THE NUMBER OF EXTERNAL INCIDENTS … AFTER THE COMPANY WENT REMOTE

30,4%

…remained the same…

7,1%

…decreased…

21,4%

…increased…

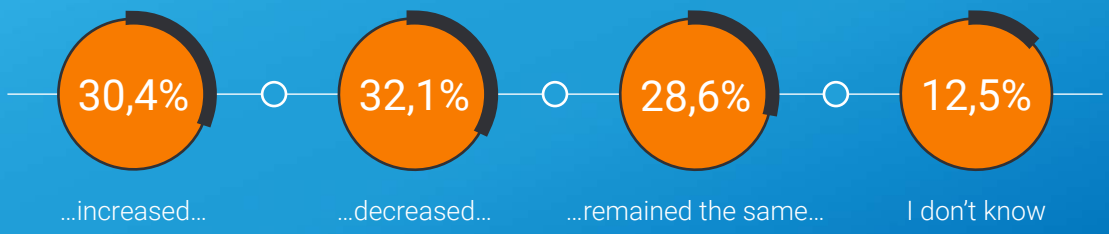
41,1%

I don't know

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

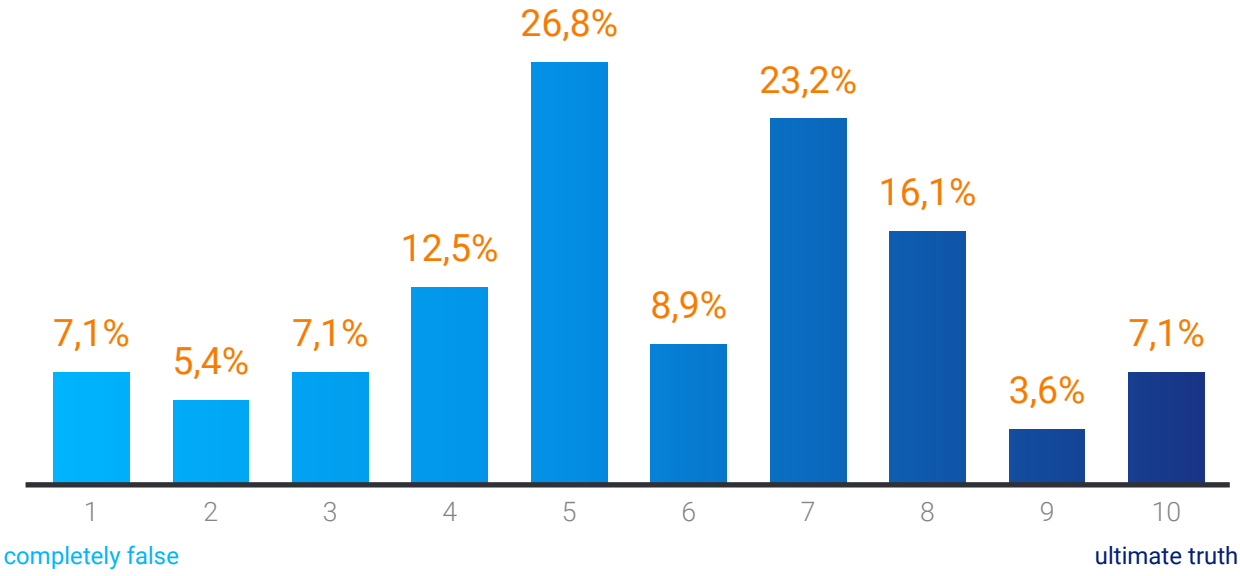
THE AMOUNT OF WORKING HOURS ... AFTER THE COMPANY WENT REMOTE



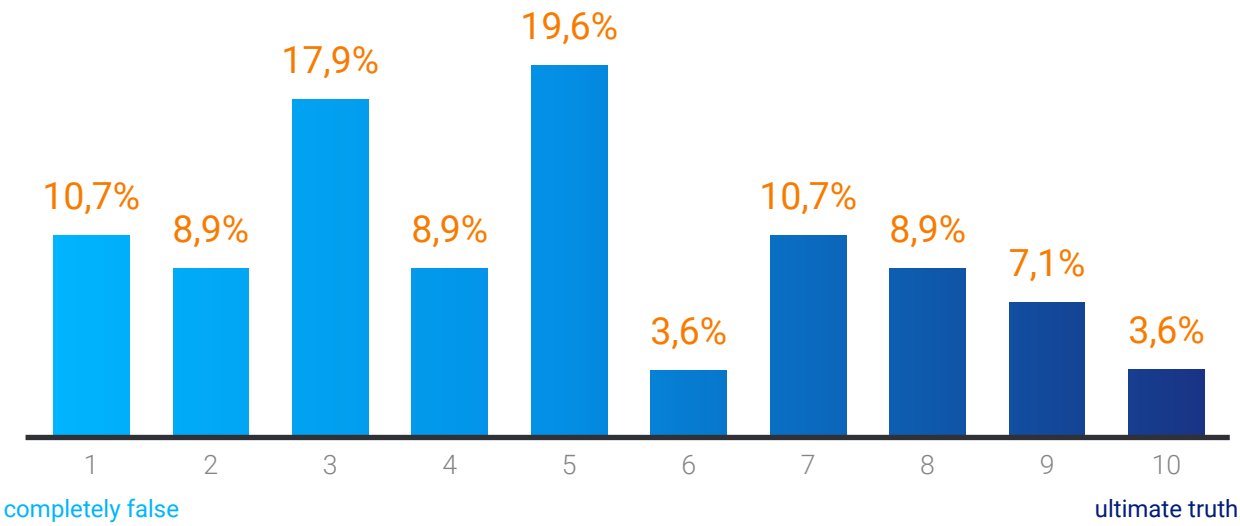
THE PERFORMANCE OF EMPLOYEES HAS ... AFTER THE COMPANY WENT REMOTE

21,4%	33,9%	25,0%	23,2%
...improved...	...dropped...	...remained the same...	I don't know

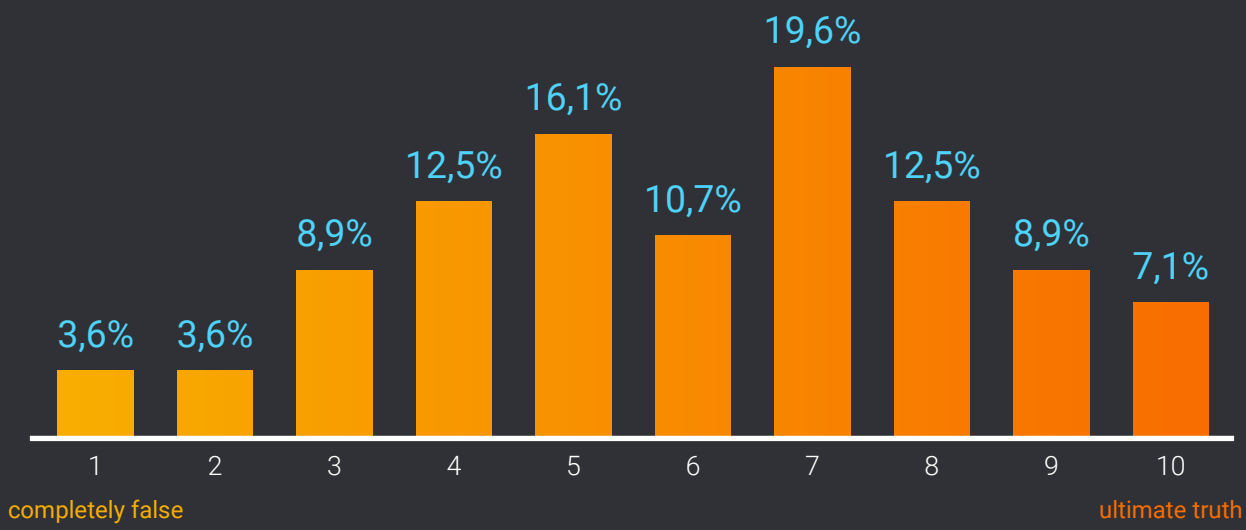
REMOTE WORK IS SAFE REGARDING INFORMATION SECURITY



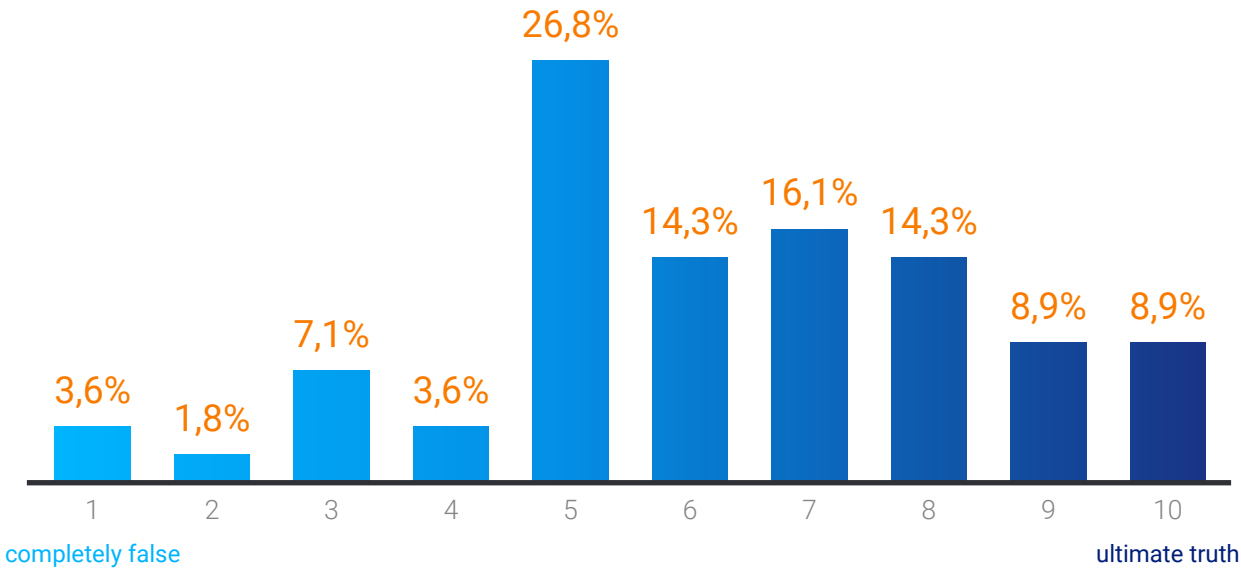
GOING REMOTE IS COSTLY



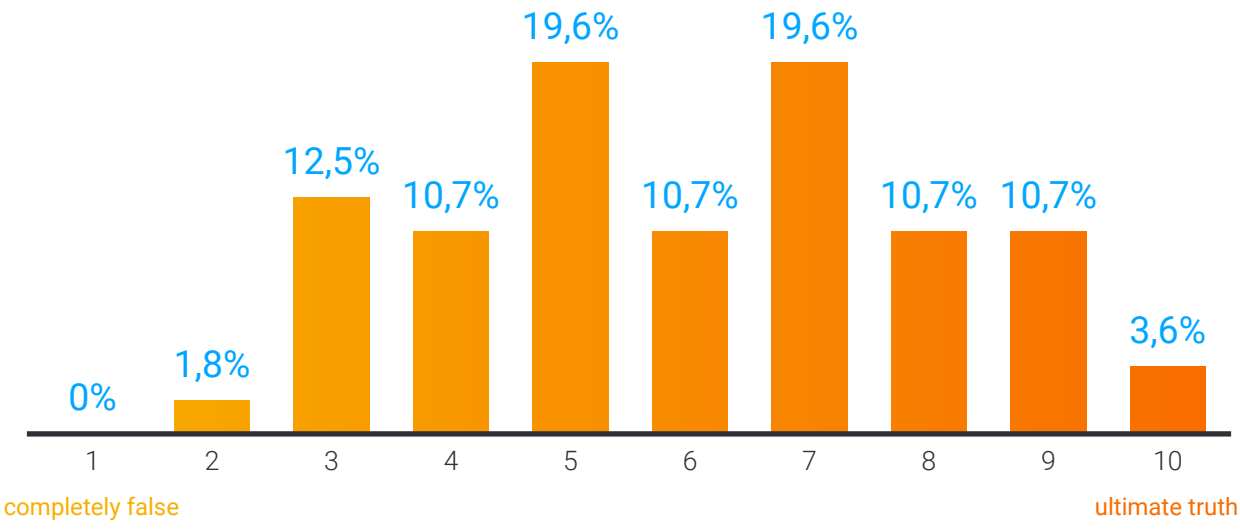
REMOTE WORK IS WORKFLOW-FRIENDLY – IS CONVENIENT FOR BUSINESS PROCESSES



MOVING TO REMOTE WORK REQUIRES EFFORTS



EMPLOYEES ARE EASILY ADAPTABLE TO WORKING REMOTELY



VPN issues, the Internet connection, user activity monitoring, software and hardware installation control as well as the new requirements which employees had to face were mentioned by the companies and appeared to be among the popular problems to deal with when going remote.

Alexey Parfentiev, leading analyst at SearchInform — developer of cyber threat mitigation solution, comments:

An emergency transition to remote work is a potentially negative process regarding data security and IT infrastructure. Those companies which have already implemented the elements of the remote format did well, and the obstacles might have been only about the scope of the problem. For the rest, moving the workflow caused difficulties — there were no resources to remodel regular processes promptly. I am glad that many companies appeared to be able to cope with the adaptation.

The situation with human resources, information and economic security is much worse — issues have faded into the background. This explains why a large number of companies have no understanding at all whether there were incidents after shifting to remote. Some said that the number of violations remained unchanged, because there is nothing to count — there are no control mechanisms. Security issues aren't of primary importance for businesses right now for obvious reasons, but the situation will surface when the number of incidents grows: an increase in the number of violations, susceptibility to social engineering attacks, BEC attacks. Therefore, companies will have to rethink their business processes in terms of security.

The respondents represent a wide range of industries, including IT, risk management and compliance, information security, banking and financial services, government, oil and gas, telecommunications, entertainment, manufacture, consulting.

We have received the opinion from small, medium and large businesses — 57% of respondents have 1–100 staff members, 25% — 100–500, 16% — 500–3000 and 2% — more than 3000 employees.