

SECURITY TRENDS BY INDUSTRY COMMUNICATIONS



40% of CPO/DPO are responsible for ownership of data privacy.



SECURITY GOVERNANCE

SECURITY BUDGET



20% of organizations have a security budget that is more than 15% of the IT budget.

69% said that board oversight of cybersecurity is the reason for increase in budget allocation.

63% said that new regulations are the reason for increase in budget allocation.



FACTORS DRIVING BUDGET

TOP INVESTMENT PRIORITY



50% said zero trust architecture is a top priority.

25% said that security orchestration and automation is a top priority.

100% agree email phishing is a top risk.

71% said cloud hosting is a top risk.



TOP 2 CYBER RISKS

SUPPLY CHAIN SECURITY



47% said they are highly confident about preventing risks from technology providers.

74% said a bad cyber event causes missed business opportunities.



CYBERATTACK CONSEQUENCES

SIMULATION EXERCISES



46% said they participate in cyberattack exercises coordinated by a third-party service provider.

38% said they participate in cyberattack exercises coordinated by National CERT/CSIRT.

15% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

- 50% said privilege escalation on cloud infrastructure has been a challenge.
- 50% said maintaining endpoint cyber hygiene has been a challenge.

TOP PRIORITIES DURING COVID-19

- Increase remote access/VPN capacity enablement
- Increased device security (EDR, etc.)

TOP PRIORITIES POST-COVID-19

- Implement zero trust architecture
- Increase secure cloud migration to scale quickly