Security priorities: a look ahead

A snapshot of how IT security leaders are prioritizing projects and planning investments in the next 12 months

Current security incidents and vulnerabilities

88%
of organizations are aware of what caused their security incidents in the past year

Top causes of security incidents

1. Employees falling victim to phishing attacks
2. Unpatched software vulnerabilities
3. Security vulnerabilities at third-party organizations or individuals
4. Misconfiguration of services or systems on or off premises
5. Unexpected business risks which exposed a vulnerability (business interruption, workforce model changes, etc.)

88%
of IT decision-makers believe their organization is falling short addressing cyber risks

Why companies are falling short addressing cyber risks

Difficulty convincing all or parts of organization of severity of risks faced	**28%**
Not investing enough resources (budget, people, tech) to address risks faced	**26%**
Struggle to find, acquire, or retain needed technical or professional expertise	**26%**

How are organizations prepping to prevent cyberattacks?

This year's top security priorities

1. Be appropriately prepared to respond to a security incident
2. Improve the protection of confidential and sensitive data
3. Upgrade IT and data security to boost corporate resiliency
4. Improve security of cloud data and systems
5. Improve/increase security awareness among end-users through training

69%
agree that understanding which security tools fit best within their company is becoming more complex

Security tools on the radar for organizations

Zero trust technologies	**32%**
SASE (Secure access service edge)	**30%**
Deception technology	**30%**
XDR (Extended Detection and Response)	**29%**
Biometrics	**28%**

Upcoming budget plans to combat risks

Top factors that will determine security spending

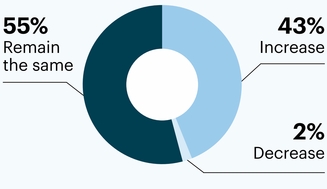
Addressing risks that result from your business's evolving use of technology	**51%**
Compliance/ regulatory mandates	**45%**
Best industry practices	**43%**

48% need additional resources from vendors during the evaluation stage of the purchase process

Increasing spend in these areas

1. Authentication
2. Data analytics
3. Cloud data protection
4. Cloud-based cybersecurity services
5. Cyber risk insurance

Security budget expectations



Artificial intelligence driving security plans

52%
of security executives agree that their organization is more likely to consider a security solution that uses AI

72% have seen benefits from the AI-enabled security technologies utilized by their organization, including:

- Faster identification of unknown threats
- Accelerated detection and response times
- AI can sift through large amounts of data faster than previous solutions

67% are leveraging AI in their security technologies, specifically in these areas:

- Threat detection
- Malware detection
- Automation alert and triage

FOUNDRY
an IDG, Inc. company

For more insight, download the executive summary.

To stay up to date on all of Foundry's findings important for tech marketers, visit https://foundryco.com/tools-for-marketers/.

Source: Foundry Security Priorities Study, 2023