FOUNDRY

Security Priorities Study 2023

Purpose and methodology

Survey goal

To gain a better understanding of the various security projects organizations are focused on now and in the coming year. The research also looks at the issues that will demand the most time and strategic thinking for IT and security teams.

Total respondents: 790

Collection method: Online questionnaire

Number of questions: 35
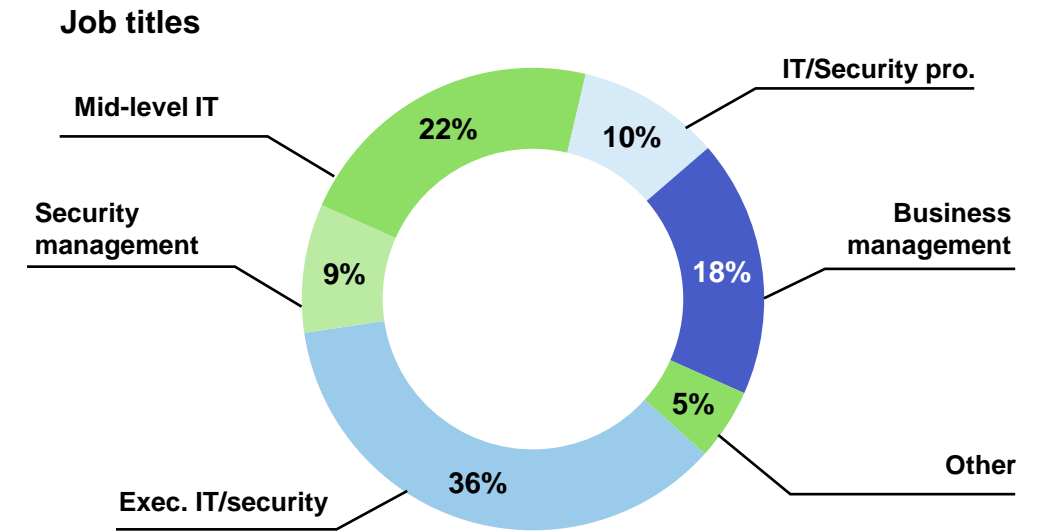
Region
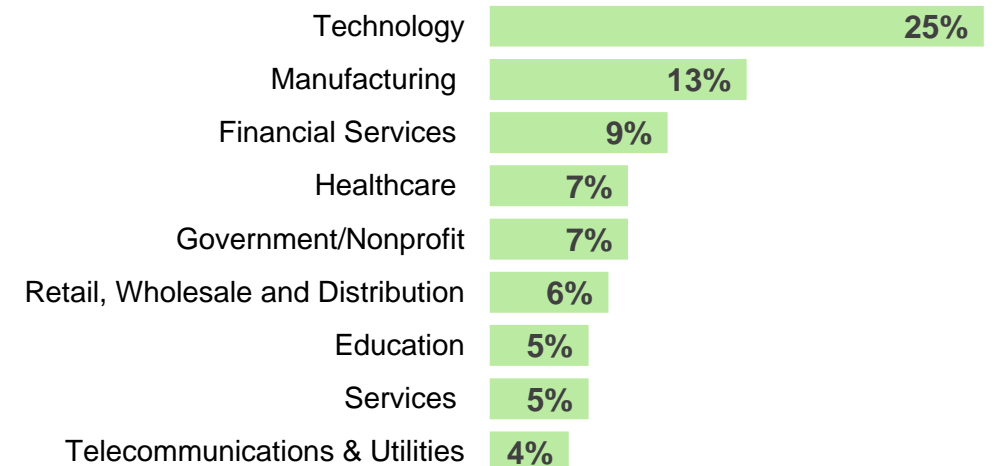**North America:** 49%
EMEA: 18%
APAC: 33%

Average company size: 11,110 employees

IT Leadership: All survey respondents are involved in IT and/or corporate/physical security decisions.

Audience base: CIO, Computerworld, CSO, InfoWorld and Network World site visitors, and email invitations to audience base

Job titles

- Mid-level IT 22%
- IT/Security pro. 10%
- Business management 18%
- Other 5%
- Exec. IT/security 36%
- Security management 9%

Top represented industries

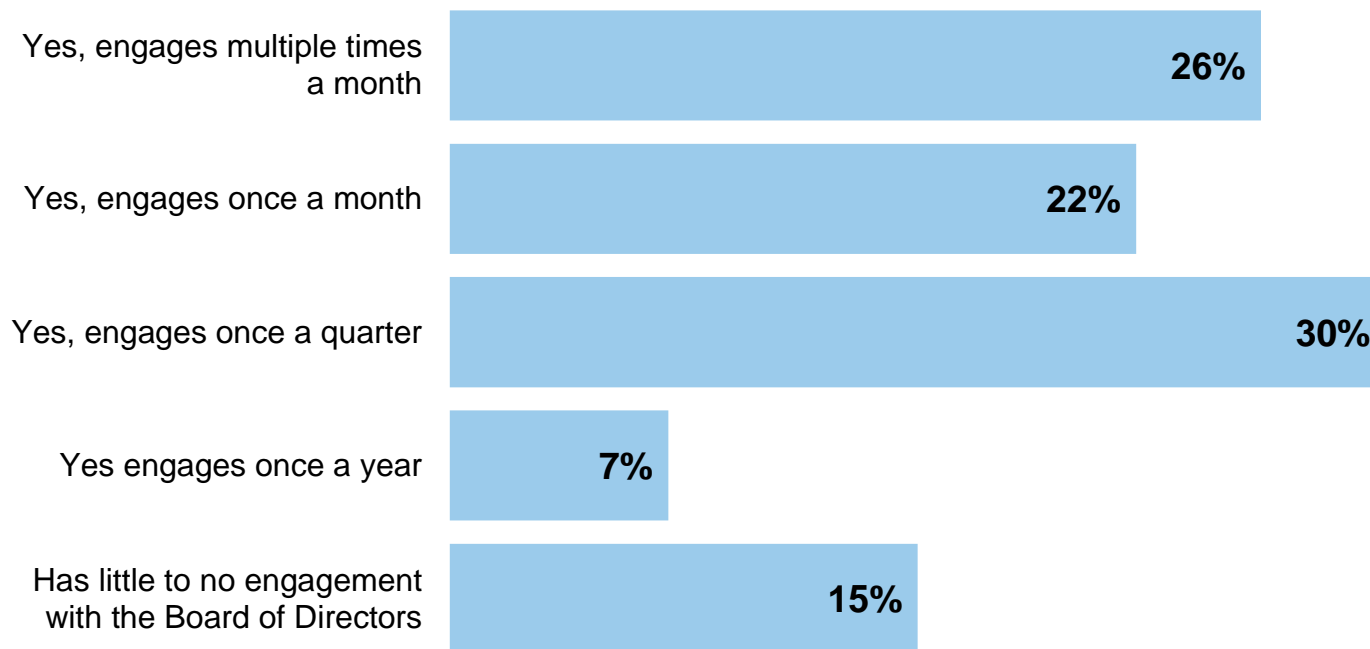| Industry	Percentage
Technology	25%
Manufacturing	13%
Financial Services	9%
Healthcare	7%
Government/Nonprofit	7%
Retail, Wholesale and Distribution	6%
Education	5%
Services	5%
Telecommunications & Utilities	4%

Engagement with Board of Directors

85%
of top IT security executives have engagement with their Board of Directors

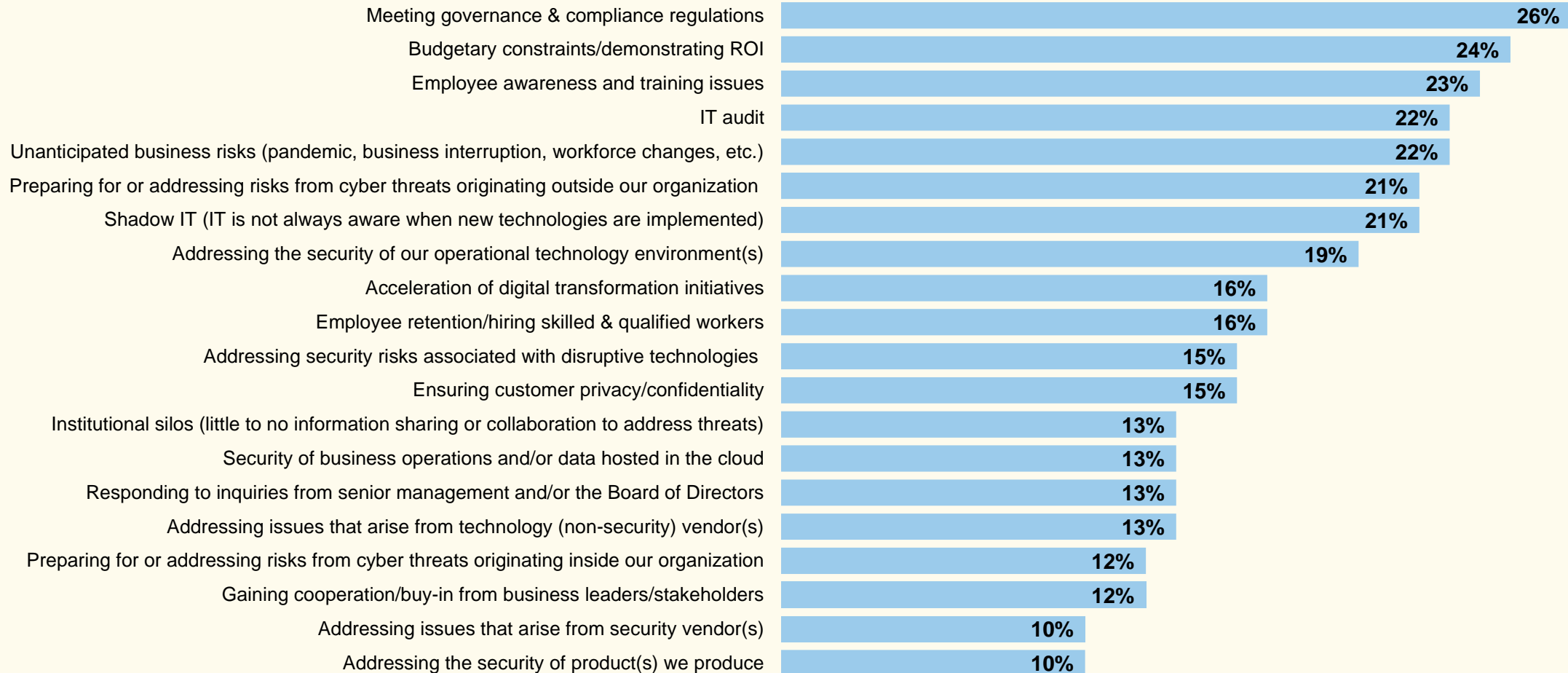|	
Yes, engages multiple times a month	26%
Yes, engages once a month	22%
Yes, engages once a quarter	30%
Yes engages once a year	7%
Has little to no engagement with the Board of Directors	15%

Question: Does your CSO/CISO/top security executive have regular engagement with the Board of Directors ?

This year's top security priorities

Priority	Percentage
Be appropriately prepared to respond to a security incident	41%
Improve the protection of confidential and sensitive data	36%
Upgrade IT and data security to boost corporate resiliency	34%
Improve security of our cloud data and systems	33%
Improve/increase security awareness among end-users through training	32%
Address risks related to OT systems, IoT devices, and/or endpoints other than computers	26%
Reduce complexity in IT security infrastructure	25%
Improve understanding of external threats	24%
Balance risk and business opportunity	23%
Enhance identity and access controls	23%
Develop a plan for leveraging AI to improve security effectiveness	21%
Respond to new security/privacy regulations	21%
Be appropriately prepared for unanticipated/unexpected risks	20%
Improve management of third-party risks	20%
Better leverage the data and analytics we collect	19%
Shorten incident response time	19%
Streamline compliance and privacy efforts	18%
Improve understanding of potential internal/insider threats	17%
Develop the next generation of security leaders	14%
Increase access to senior business leadership	7%

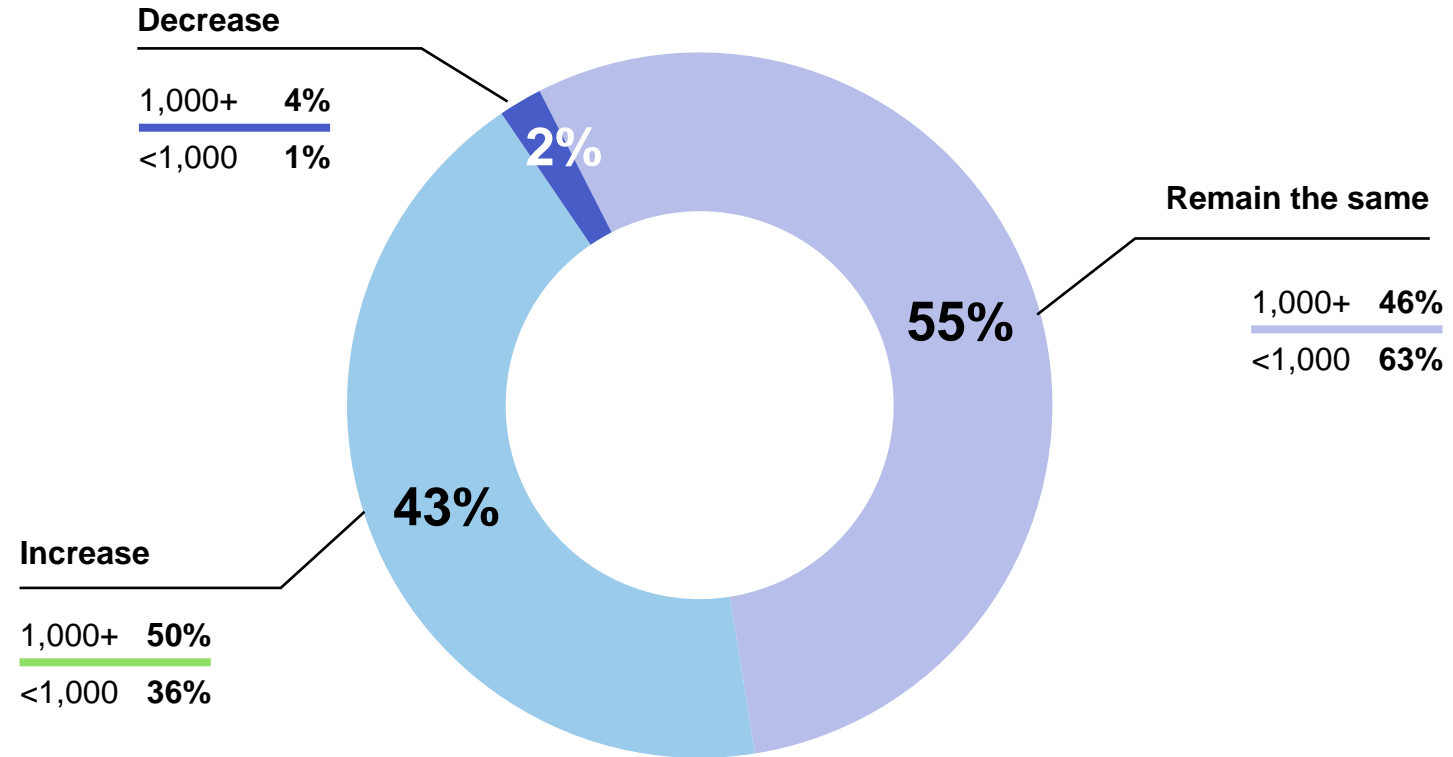**Question:** What are your organizations top security priorities for the coming year?

Challenges forcing security leaders to redirect their time

Challenge	Percentage
Meeting governance & compliance regulations	26%
Budgetary constraints/demonstrating ROI	24%
Employee awareness and training issues	23%
IT audit	22%
Unanticipated business risks (pandemic, business interruption, workforce changes, etc.)	22%
Preparing for or addressing risks from cyber threats originating outside our organization	21%
Shadow IT (IT is not always aware when new technologies are implemented)	21%
Addressing the security of our operational technology environment(s)	19%
Acceleration of digital transformation initiatives	16%
Employee retention/hiring skilled & qualified workers	16%
Addressing security risks associated with disruptive technologies	15%
Ensuring customer privacy/confidentiality	15%
Institutional silos (little to no information sharing or collaboration to address threats)	13%
Security of business operations and/or data hosted in the cloud	13%
Responding to inquiries from senior management and/or the Board of Directors	13%
Addressing issues that arise from technology (non-security) vendor(s)	13%
Preparing for or addressing risks from cyber threats originating inside our organization	12%
Gaining cooperation/buy-in from business leaders/stakeholders	12%
Addressing issues that arise from security vendor(s)	10%
Addressing the security of product(s) we produce	10%

Question: What security-related challenges are most often forcing you to redirect your time and focus away from more strategic tasks?

Source: Foundry Security Priorities Study, 2023

Security budget expectations

Decrease

1,000+	**4%**
<1,000	**1%**

2%

Remain the same

1,000+	**46%**
<1,000	**63%**

55%

43%

Increase

1,000+	**50%**
<1,000	**36%**

Question: Do you expect your organization's overall security budget to increase, decrease or remain the same in the next 12 months?

Complexity emerges around security investments

69%

agree that understanding which security tools and solutions fit best within our company is becoming more complex

52%

agree that their organization is more likely to consider a security solution that uses Artificial Intelligence (AI)
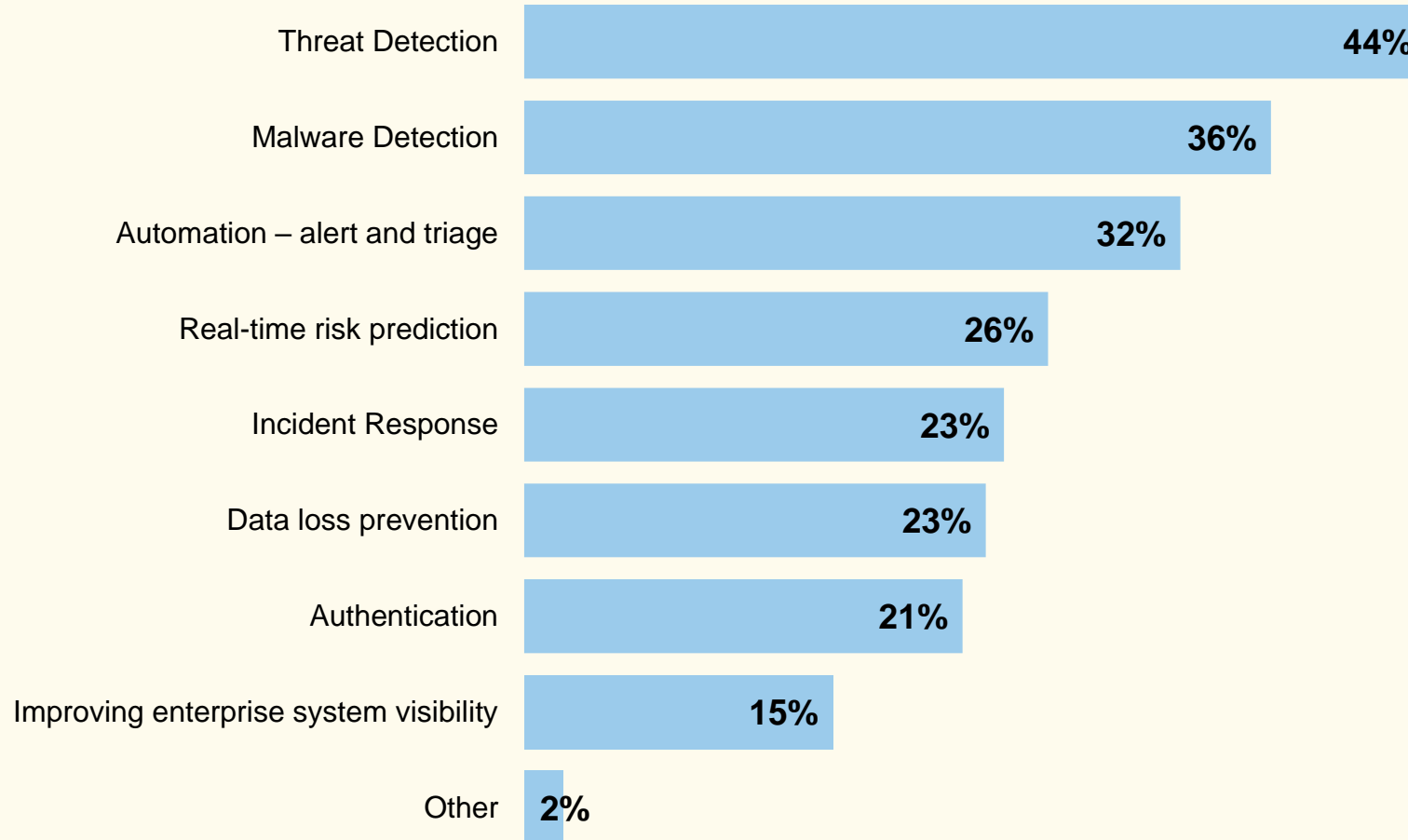
49%

agree that their responsibilities include addressing information security issues outside of my country or region

Question: Please rate your level of agreement with the following statements:

Leveraging AI in security technologies

Threat Detection	**44%**
Malware Detection	**36%**
Automation – alert and triage	**32%**
Real-time risk prediction	**26%**
Incident Response	**23%**
Data loss prevention	**23%**
Authentication	**21%**
Improving enterprise system visibility	**15%**
Other	**2%**

67%

are leveraging Artificial Intelligence in their security technologies

1,000+	**79%**
<1,000	**55%**

Question: In which areas are you leveraging Artificial Intelligence (AI) in your security technologies?

Conclusions

To assist with their initiatives, top security execs have regular engagement with their Board of Directors. Many says this helps and that their Board has experience with cybersecurity-related issues.

But there is always room for improvement, as 88% believe their organization is falling short in addressing cyber risk, specifically when it comes to convincing their organization of the severity of the risks they face.

IT leaders are addressing these security risks by investing in new solutions and increasing spend on what they have in their current security stack.

98% of security leaders say they expect their security budgets to either increase or remain the same over the next 12 months.

They are spending their money on things like cyber insurance polies and are starting to leverage artificial intelligence in their security tech.