2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

Data Governance in Digital Transformation

Insights on Skills Gap and Talent Training

David Samuelson, CEO
ISACA

AGENDA

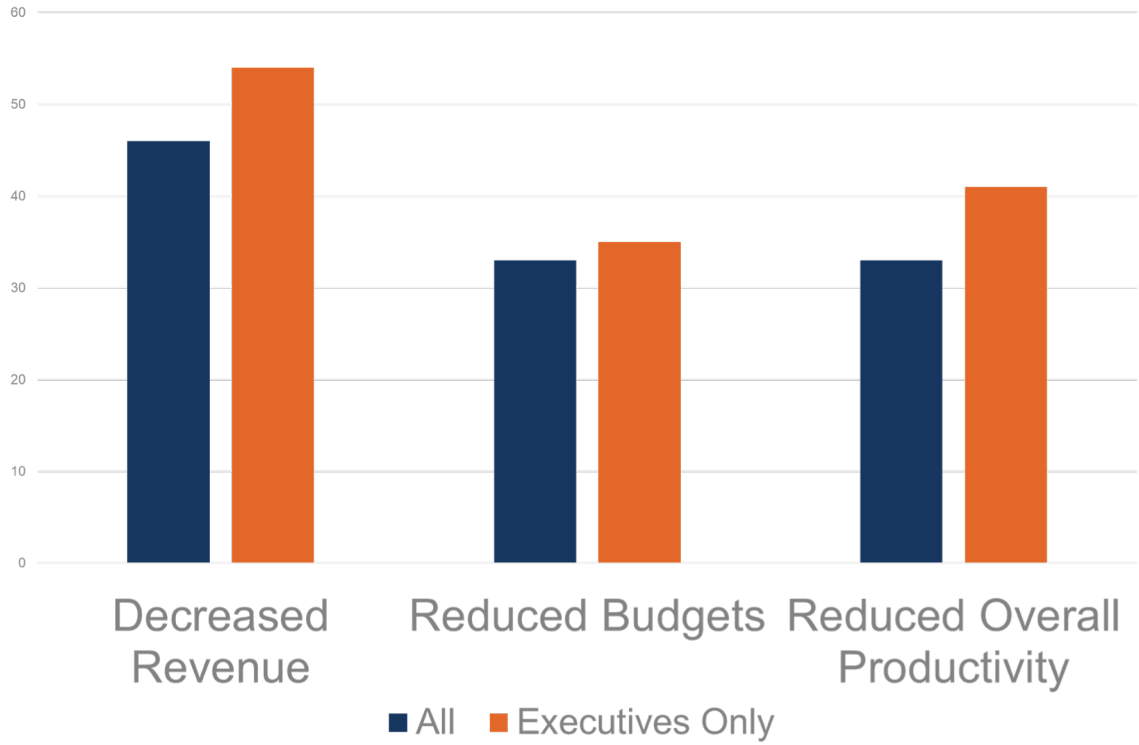
- COVID-19 Impact
- Growing Opportunities – and Threats
- Rethinking Data Governance & Management
- Data Management & Maturity Model (DMM)
- 2020 State of Cybersecurity: Threats and Skills Gaps
- Tech Workforce 2020 Research
- Staffing and Organization Impact Outcomes
- Closing the Skills Gap

Has your organization experienced any of the following as a result of the COVID-19 pandemic?

Decreased revenues
46% All
54% Executives

Reduced budgets
33% All
35% Executives

Reduced overall productivity
33% All
41% Executives



Source: COVID-19 Study: ISACA Professionals Weigh in on Impact and Outlook, April 2020

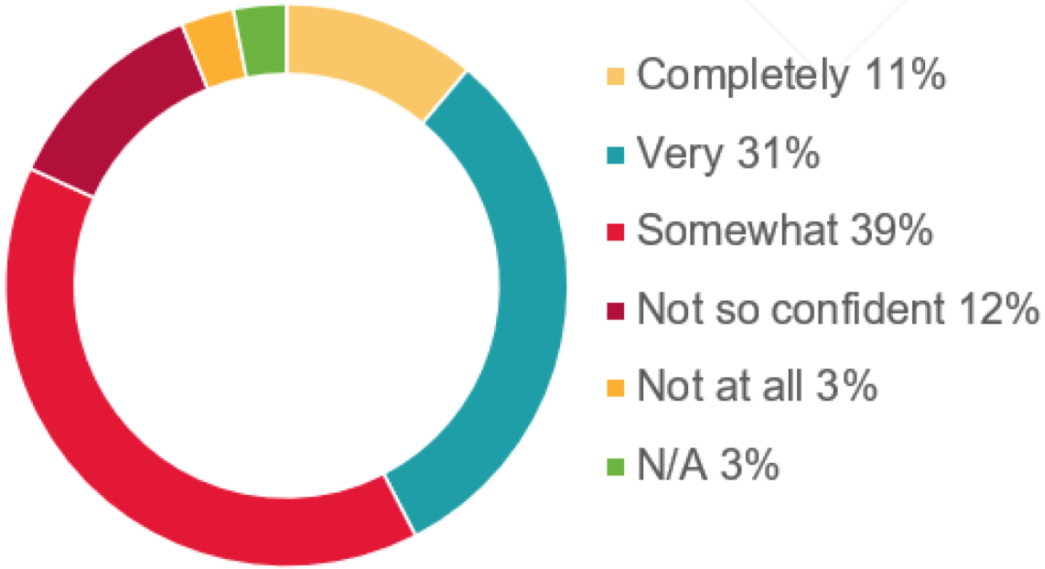
ISACA RESEARCH: EXECUTIVE VIEWS ON COVID-19 IMPACT

How much impact will COVID-19 have on your organization’ s risk?

SIGNIFICANT RISK
Financial (43%)

MODERATE RISK
Operational
Strategic
Cybersecurity
Talent

MINIMAL RISK
Technology
Political
Compliance/Legal
Reputational

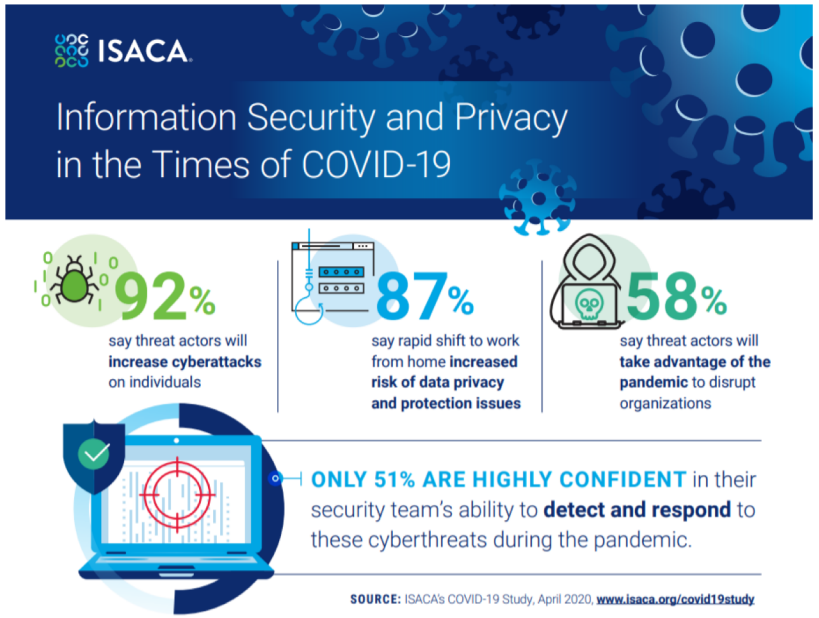


How confident are you in your organization’ s ability to detect and respond to privacy breaches during the COVID-19 pandemic?

Source: COVID-19 Study: ISACA Professionals Weigh in on Impact and Outlook, April 2020

ISACA COVID-19 RESOURCE CENTER

www.isaca.org/go/covid19



CRISIS MANAGEMENT AND BUSINESS CONTINUITY

Blog Post

COVID-19 Underscores Value of Resilient Supply Chains

My supply chain focus started when I was the vice president controller for a shoe retailer in...

23 June 2020

Article

Evaluating Business Service Continuity and Availability Using COBIT...

COBIT 2019's enterprise goal EG06 Business service continuity and availability mus...

1 June 2020

Podcast

Information Systems in the Time of Pandemic

Many organizations found themselves unprepared for the workplace and business...

30 April 2020

Blog Post

Business Continuity – Pandemic Preparation

The recent outbreak of a new virus, COVID-19, or the coronavirus, has many...

3 March 2020

Moving Toward New Ways of Doing Business

"Organizations are rapidly and aggressively moving toward new ways of doing business during this time, which is a very positive thing, but it can also lead to making compromises that can leave them vulnerable to threats. A surge in the number of remote workers means there is a greater attack surface. Remote work is critically important right now, so security has to be at the forefront along with employee education. ISACA professionals have an especially critical role to play in protecting their enterprises, customers and stakeholders during this pandemic."

– David Samuelson, ISACA CEO

REMOTE WORK

Blog Post

Tailoring Enterprise Information Security Training and Awareness...

The ongoing COVID-19 outbreak has compelled most organizations to roll out work...

14 July 2020

Article

Five Key Considerations When Securing a Work-from-Home Workforce

Recent events have forced many organizations to require their workforces to operate...

6 July 2020

Blog Post

Telework Successfully During (And After) the COVID-19 Pandemic

For state/province/national leaders, coronavirus is forcing a trade-off between public healt...

5 May 2020

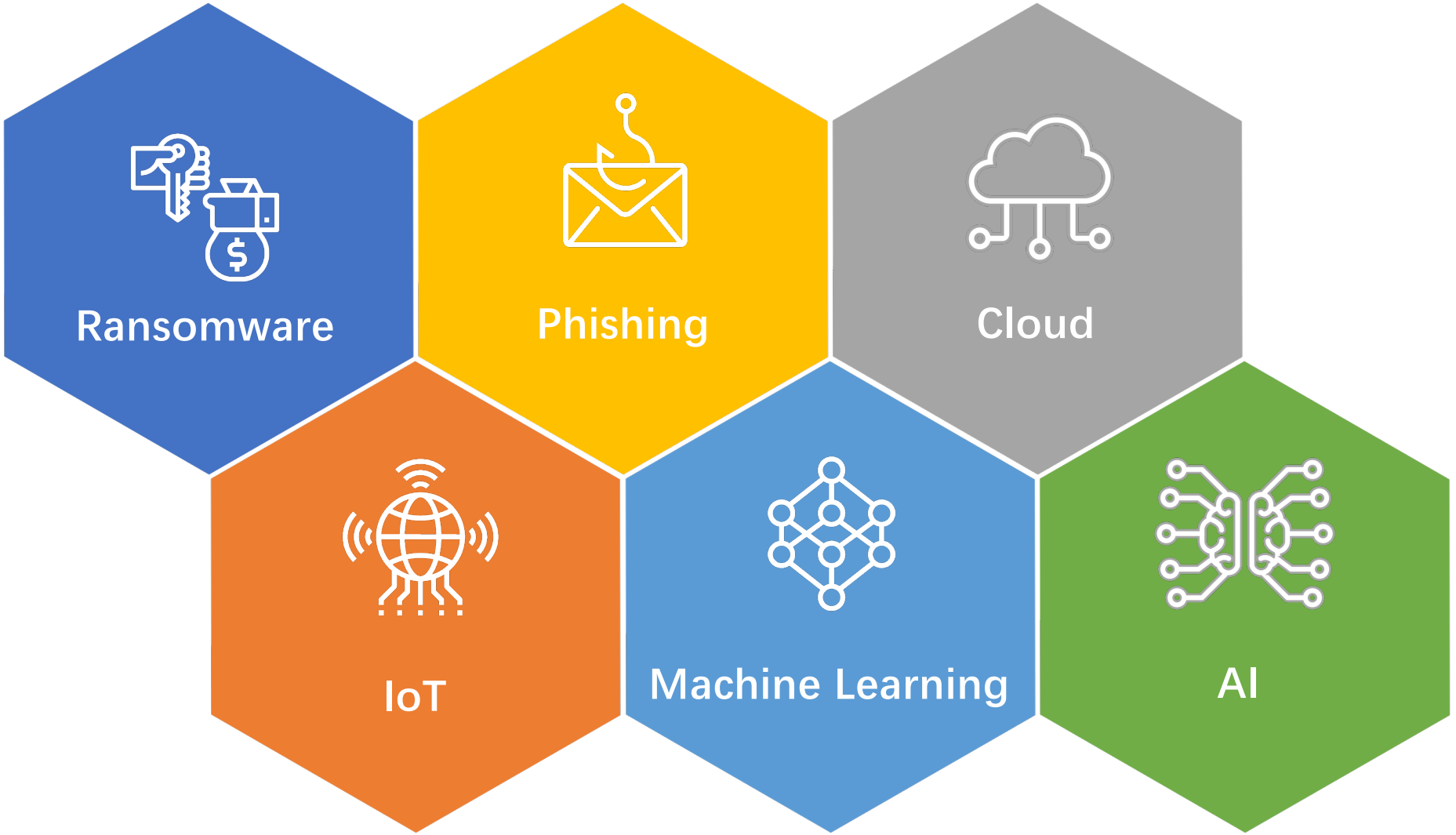
Article

Managing Remote Work Environments With COBIT 2019

More organizations are making the shift to remote working environments for their...

30 March 2020

GROWING OPPORTUNITIES – AND THREATS



内 容

Free download in Chinese and English:

www.isaca.org/bookstore/bookstore-wht_papers-digital/whprdg

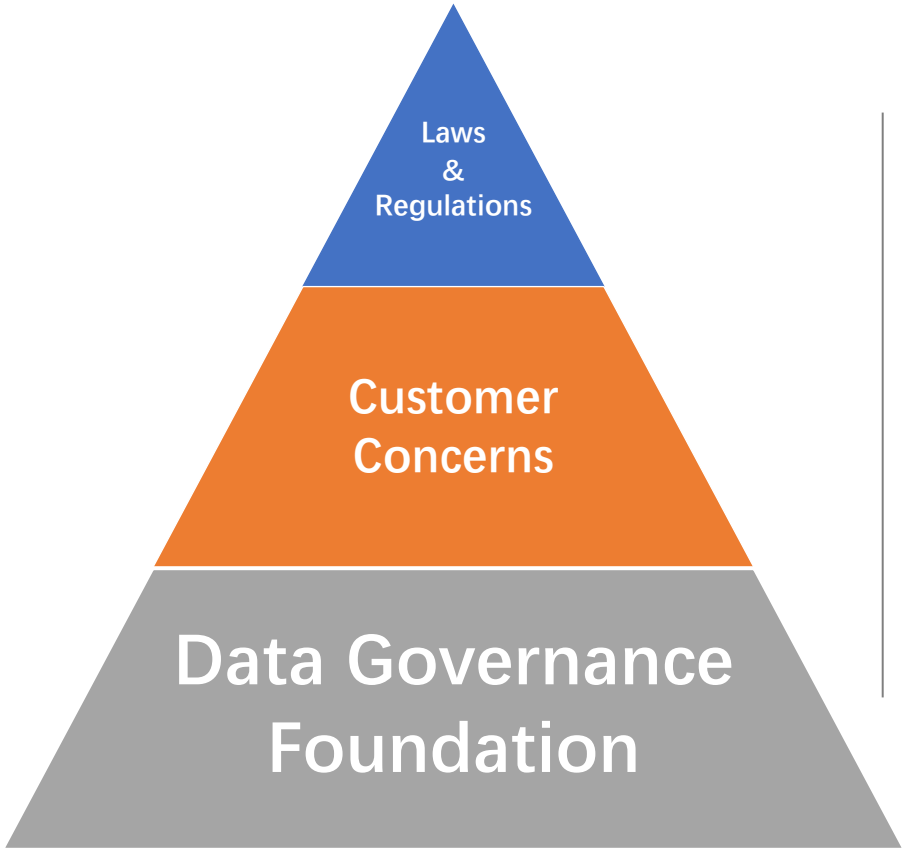
EMBEDDED DATA GOVERNANCE

Develop & Embed data governance

Clarify policies & standards

Define roles & responsibilities

DATA GOVERNANCE FOUNDATION



Phase 1

Design and Deploy a Data Governance Strategy

Phase 2

Implement a Data Management Platform

What data does your organization **have and need** to use?

When are data governance practices taking place through your organization’ s data life cycle?

Who is responsible for your organization’ s governance?

How will data be managed in your organization?

STORYTELLING FOR BETTER BUSINESS RESULTS

Free download in English or Chinese: cmmiinstitute.com/data-management-maturity

5 STEPS TOWARD DATA MANAGEMENT

Beyond the Basics

Defining Data Management

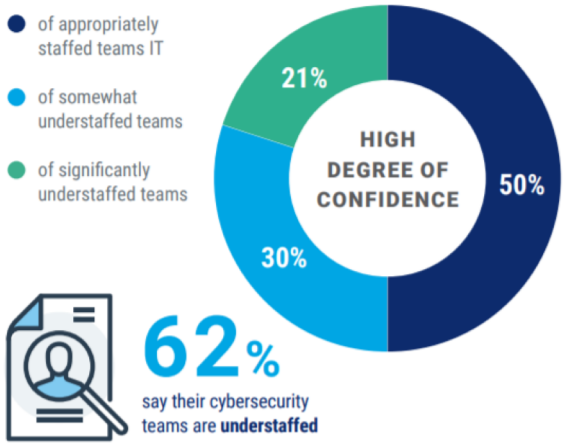
Make Smarter Decisions

Measure Your Success

Bring Clarity To Business Goals

2020 STATE OF CYBERSECURITY: THREATS

Fully Staffed Teams Are More Confident in Their Ability to Respond to Cyberthreats



62% say their cybersecurity teams are **understaffed**

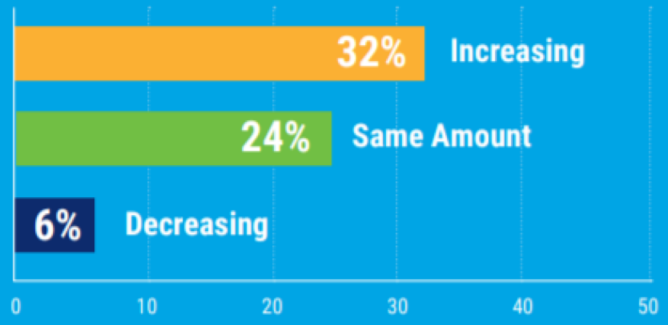
MOST FREQUENT
Attack Methods

1. **Social engineering** (15%)
2. **Advanced persistent threat** (10%)
3. **Ransomware and unpatched systems** (9% each)

HIRING TIME MATTERS
Those who take longer to fill positions also report more attacks:

MORE CYBERATTACKS THIS YEAR	TIME TO FILL CYBER POSITION
26%	Less than two weeks
35%	3 months
38%	Six months or more
42%	Cannot fill

Cyberattacks Are Still Increasing Year Over Year



https://www.isaca.org/go/state-of-cybersecurity-2020

2020 STATE OF CYBERSECURITY: WORKFORCE

2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

32%

say it takes six months or more to fill an open cybersecurity position with a qualified candidate

70%

say fewer than half of cybersecurity applicants are well qualified

72%

of cybersecurity professionals believe that their HR department **does not regularly understand** the needs

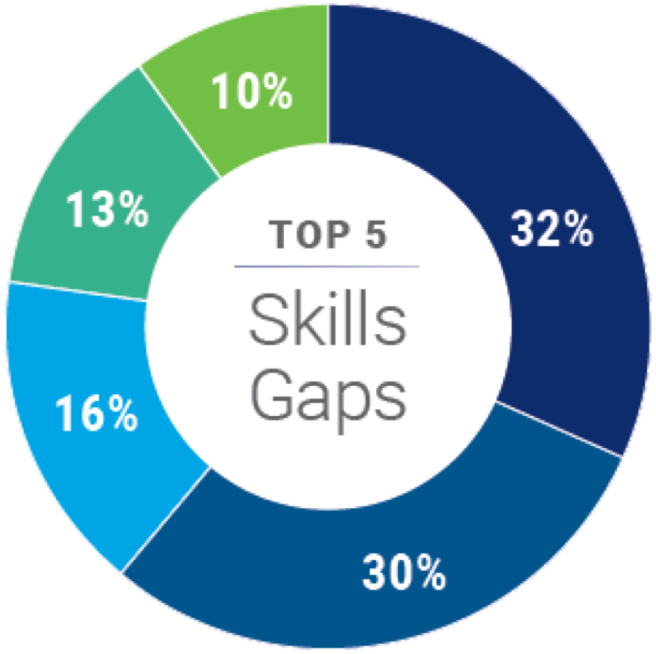
62%

say their organization's cybersecurity team is **understaffed**

57%

say they currently have **unfilled** cybersecurity positions on their team

Skills Gaps Persist



- Soft skills
- IT knowledge and skills gaps
- Insufficient business insight
- Cybersecurity technical experience
- Insufficient hands-on training

Retention Concerns Increase

TOP 5 REASONS

Respondents say cybersecurity staff are leaving:

1. **59%** Recruited by other companies
2. **50%** Limited promotion and development opportunities
2. **50%** Poor financial incentives
3. **40%** High work stress levels
4. **39%** Lack of management support

66% say it's **difficult** to retain cybersecurity talent (an increase from last year)

70%

Consider themselves in-play for being recruited

64% SAY THEY EXPERIENCE STRESS OR BURNOUT IN THEIR CURRENT ROLES DUE TO:

- Heavy workloads
- Long hours
- Lack of resources

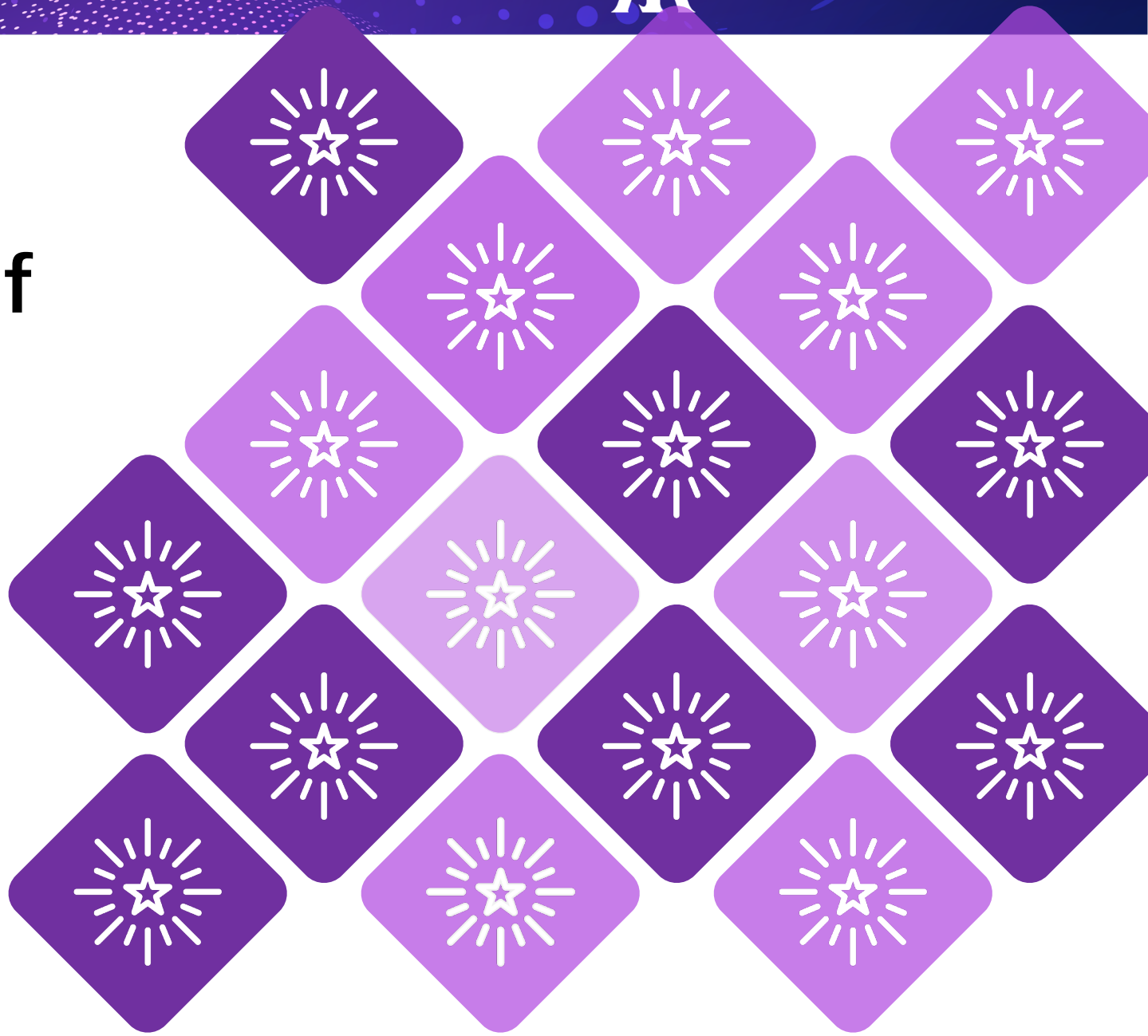
TOP 5 CAREER ADVANCEMENT OBSTACLES:

- Limited access to career growth opportunities
- Lack of mentors
- Unequal growth opportunities
- Lack of resources for training
- Unsupportive management

STAFFING AND ORGANIZATION IMPACT OUTCOMES

Who is the accountable owner of security at your enterprise?

Do you have an appropriate commitment to security?



CLOSING THE SKILLS GAP

LIFELONG LEARNING

INVEST IN TEAMS

EVOLVE SKILLS

2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音