

Current & Present Dangers in the Cloud

CISO Cloud Summit Italy

PRESENTED BY



Illena Armstrong
President, Cloud Security Alliance
November 30, 2021



2021 SO FAR:



Public Cloud Spending Grows

Gartner Forecast, November 2020



Almost 70% of organizations using cloud services plan to increase cloud spending after Covid-19-related disruptions.



2021:

Worldwide end-user spending on public cloud services to grow 18.4%.

TOTAL:

\$304.9 billion,
up from \$257.5 billion in 2020



14.2% of total global enterprise IT spending will be dedicated to cloud in 2024, up from 9.1% in 2020.

Growth in Public Cloud through 2024

Enterprises will increase investments in:

- **mobility**
- **collaboration**
- **other remote working technologies**
- **infrastructure**

Still more market expansion is likely as cloud service providers continue partnering with telecommunications companies to extend their reach into the edge & support hybrid workforces.

Gartner, November 2020

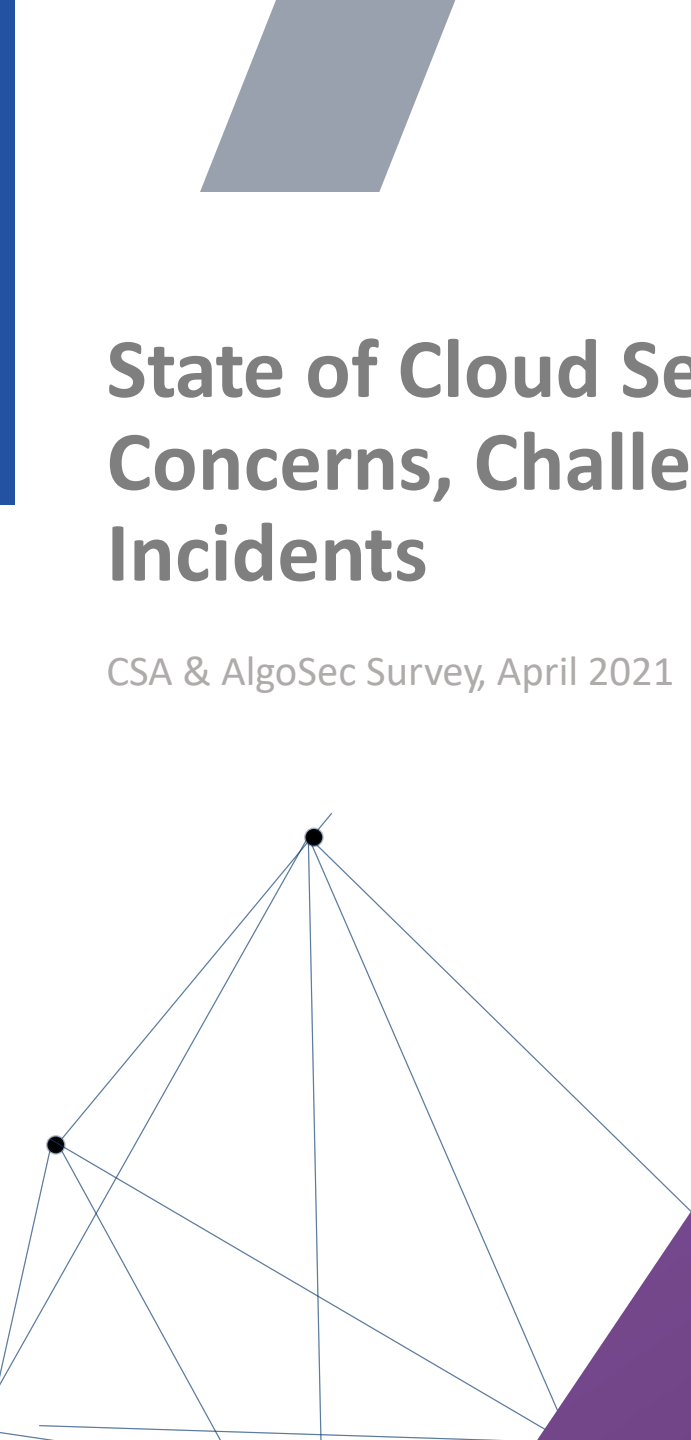
Growth spurts

Software as a Service (SaaS) is largest market segment & is forecasted to grow to \$117.7B in 2021

Platform as a Service (PaaS) or application infrastructure services to grow at even higher margins

**Main Driver:
Remote workers' need for high performing,
content-rich & scalable infrastructure**

Gartner, November 2020



State of Cloud Security Concerns, Challenges and Incidents

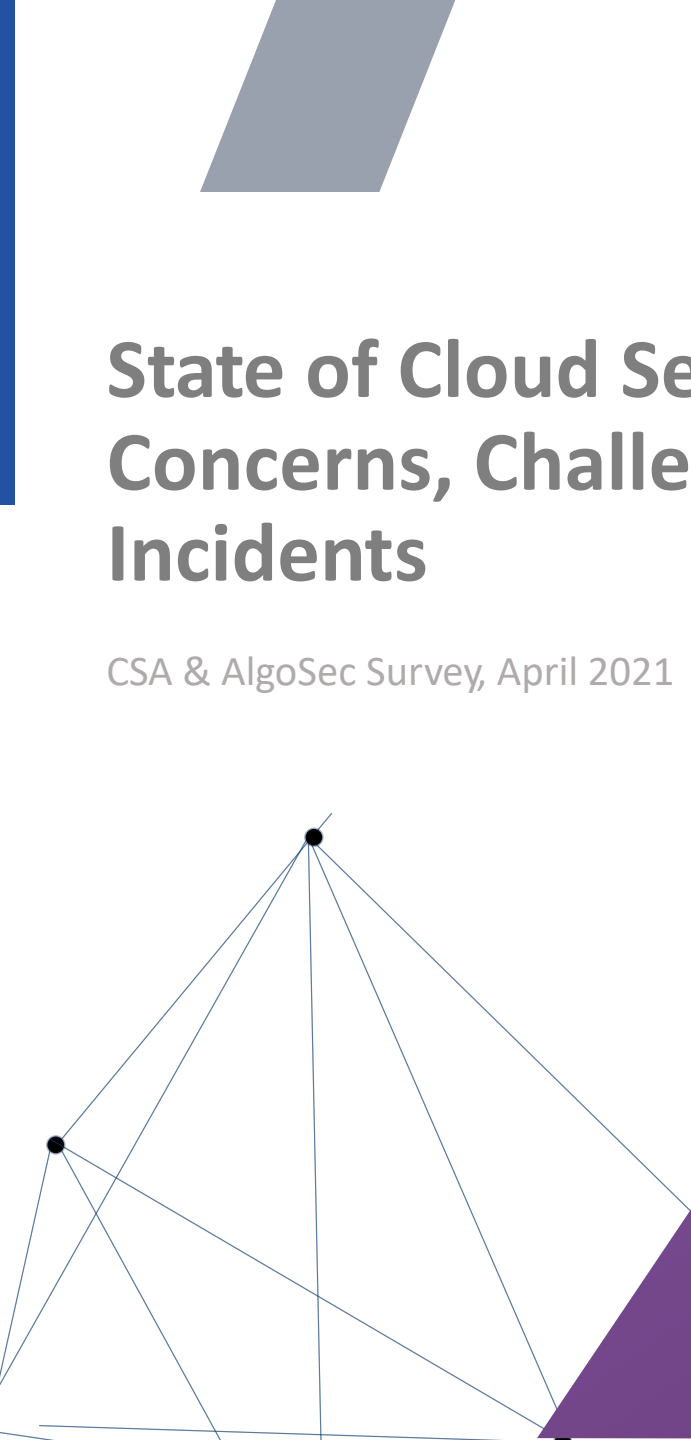
CSA & AlgoSec Survey, April 2021

62%

Have a multi-cloud strategy,
with 27% using 3 or more public
cloud platforms.

67%

Market Share Evenly Spread
Though AWS is the frontrunner, with Azure
a close second at 65%.



State of Cloud Security Concerns, Challenges and Incidents

CSA & AlgoSec Survey, April 2021

>50%

Are running 41% or more of
their workloads in a public
cloud, up from 25% in 2019.

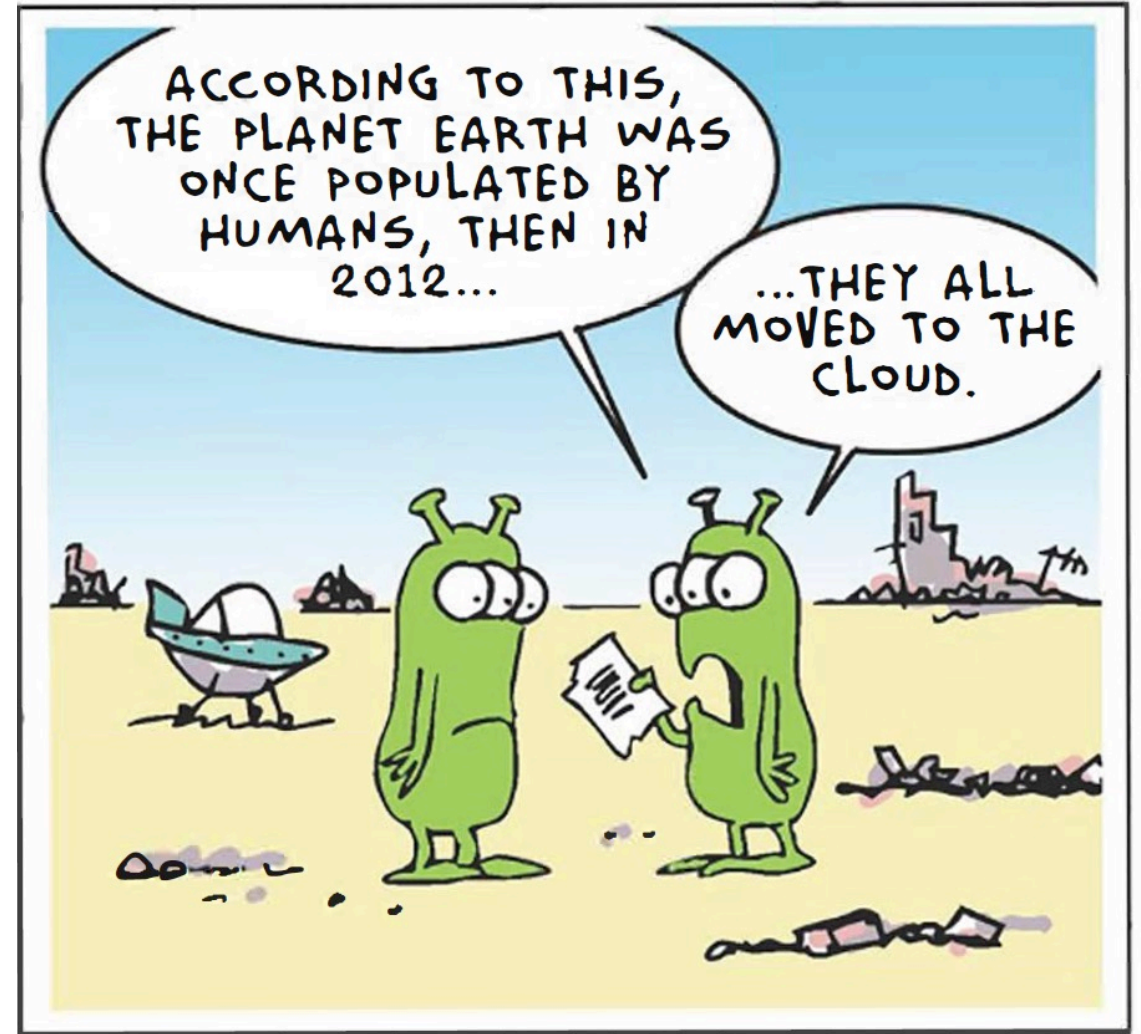
63%

Expect to run 41% or more of
their workloads in a public
cloud this year.

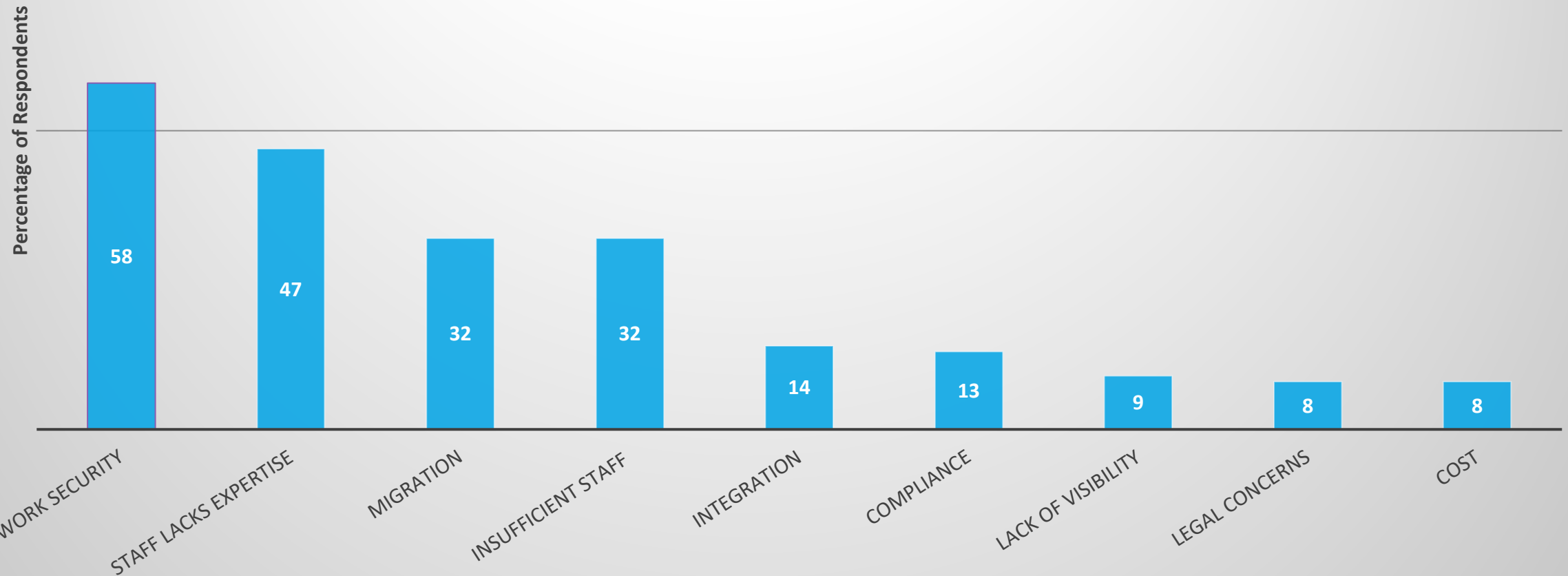
Reasons for Increased Moves to the Cloud

- Reduced Cost
- Increased Agility & Elasticity
- DevOps-Friendly
- Improved Uptime

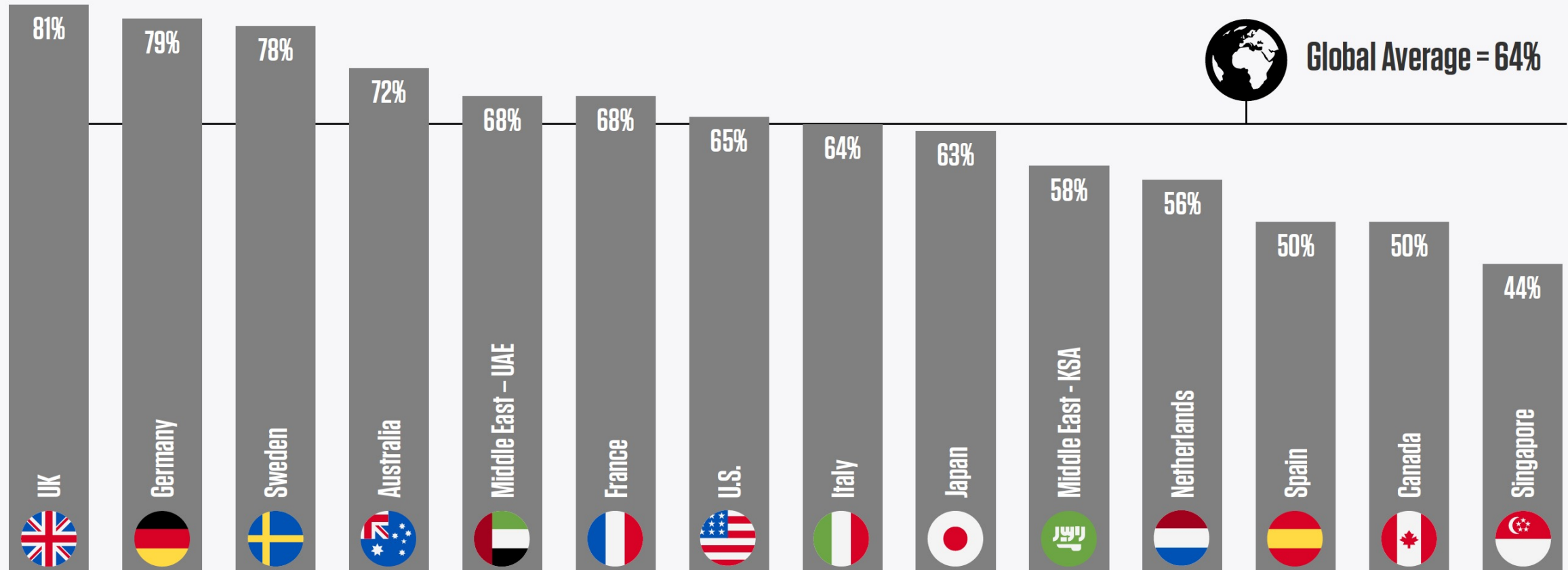
On average, respondents say providers are meeting or even exceeding expectations.



Cloud Security Concerns

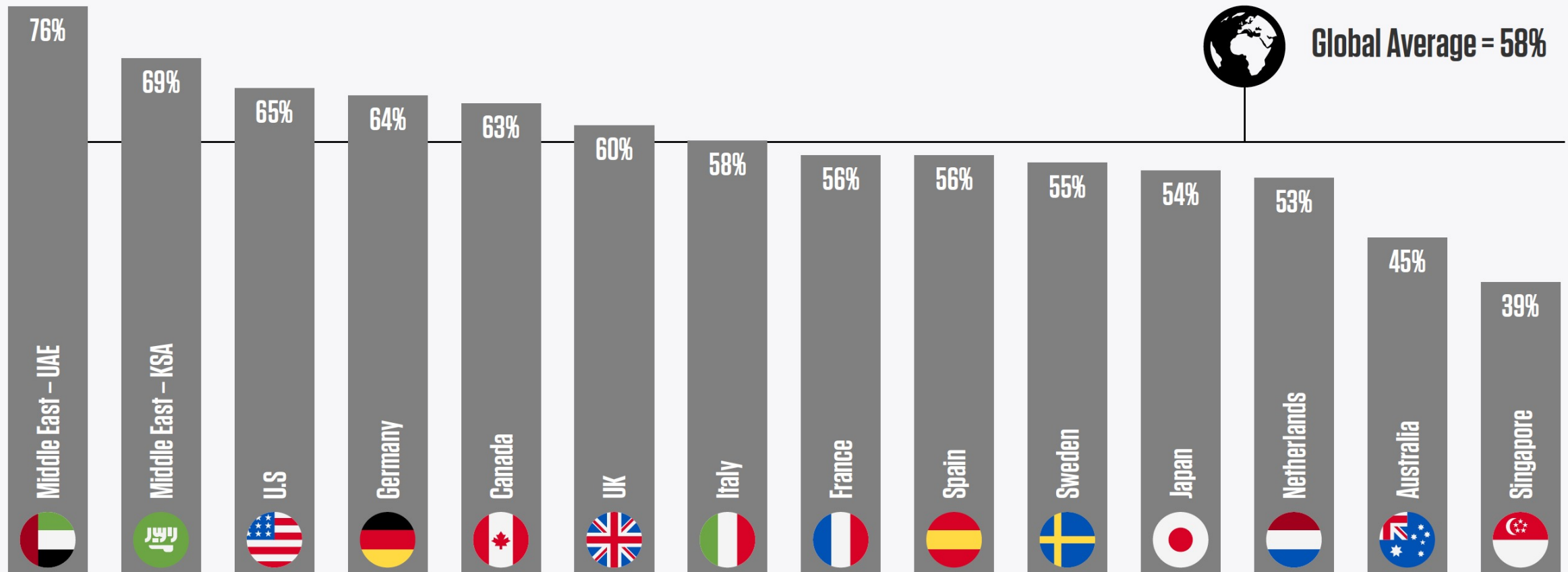


Percentage of CISOs in agreement that their organization is at risk of a material cyber attack in the next 12 months

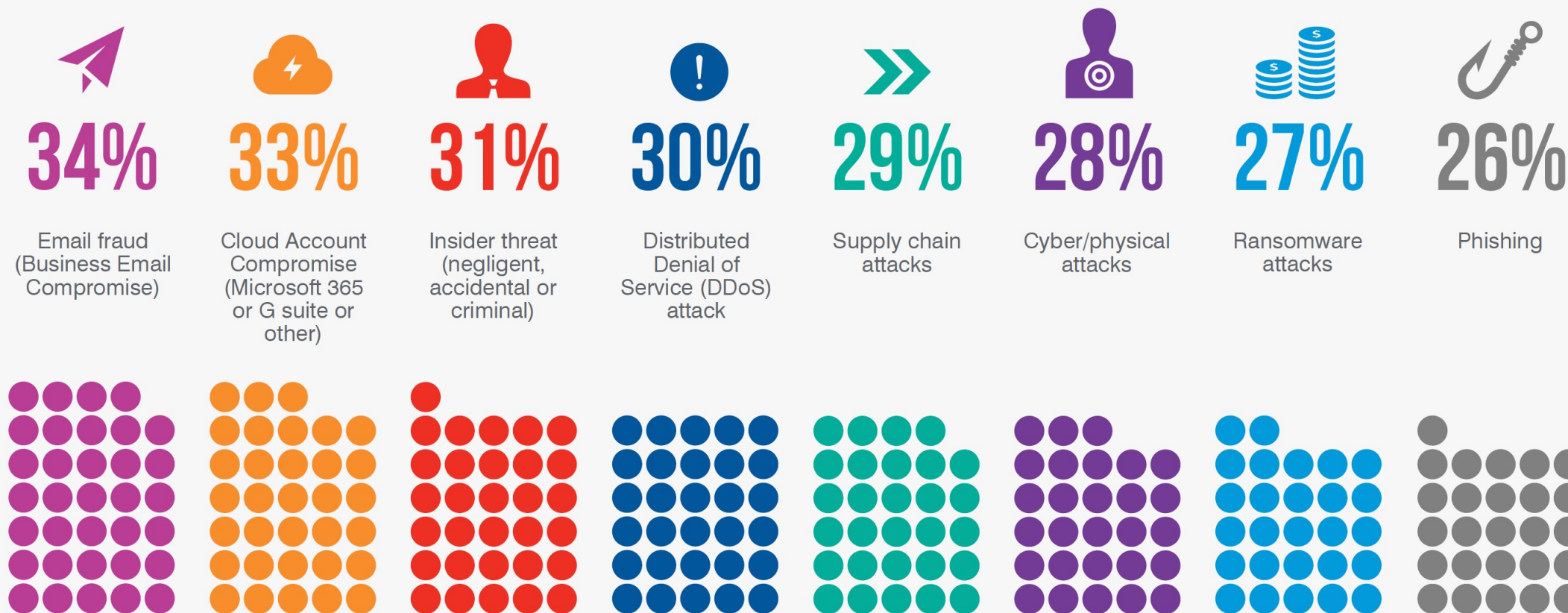


Proofpoint 2021 – Voice of the CISO
Research Survey Report

Percentage of CISOs saying their business has seen more targeted attacks since enabling widespread remote working



Perceived Biggest Cybersecurity Threats in the Next Year



*Proofpoint 2021 – Voice of the CISO
Research Survey Report*



Business Email Compromise

12 out of 14 surveyed countries consider BEC a **top 3 risk**.



BEC is considered the **number 1** risk in Canada, Sweden, Spain, and Japan.



Cloud Account Compromise

10 out of 14 surveyed countries consider Cloud Account Compromise a **top 3 risk**.

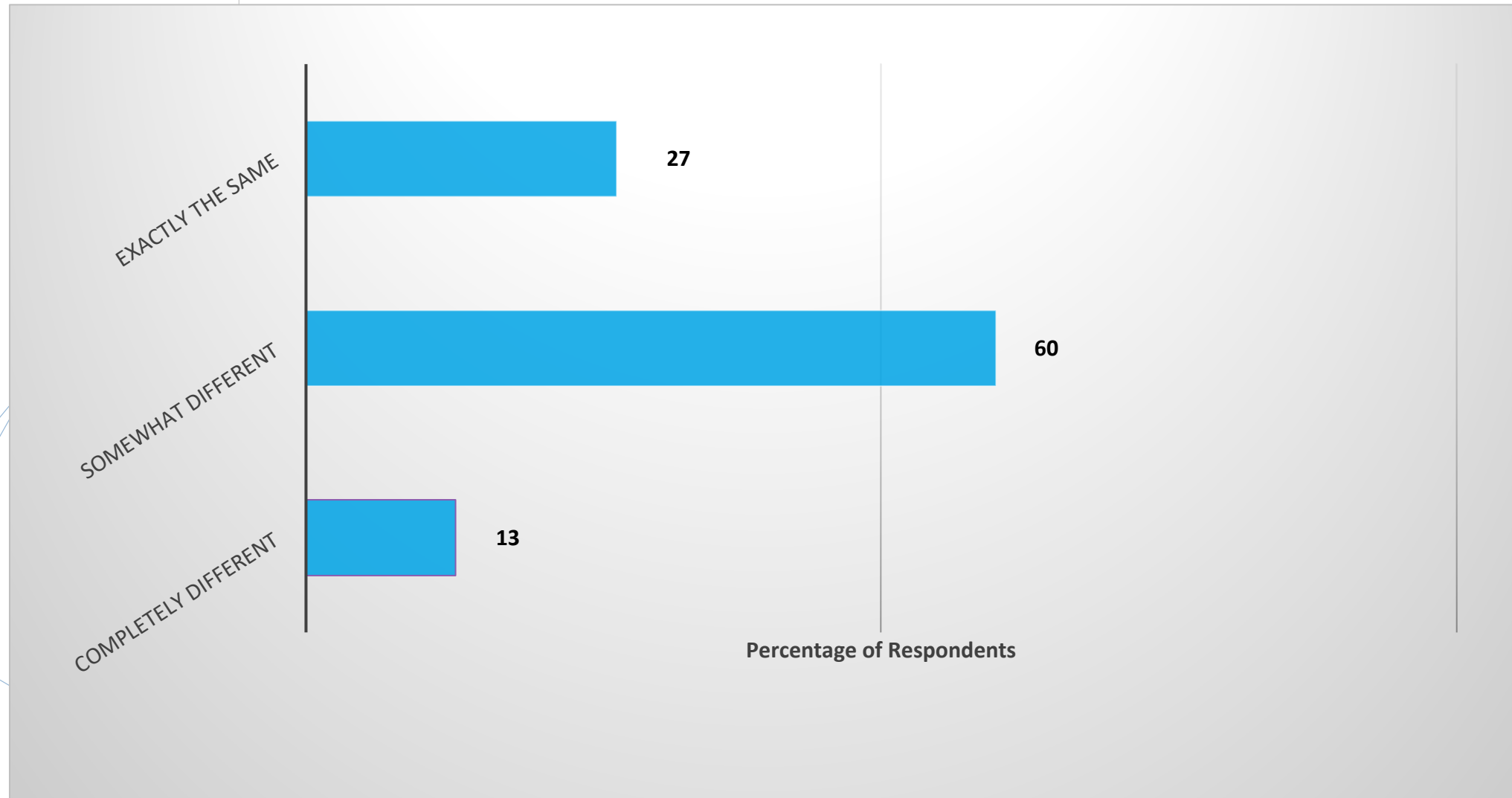


Cloud Account Compromise is the **number 1** risk in the U.S., France, Italy, and Saudi Arabia (KSA).

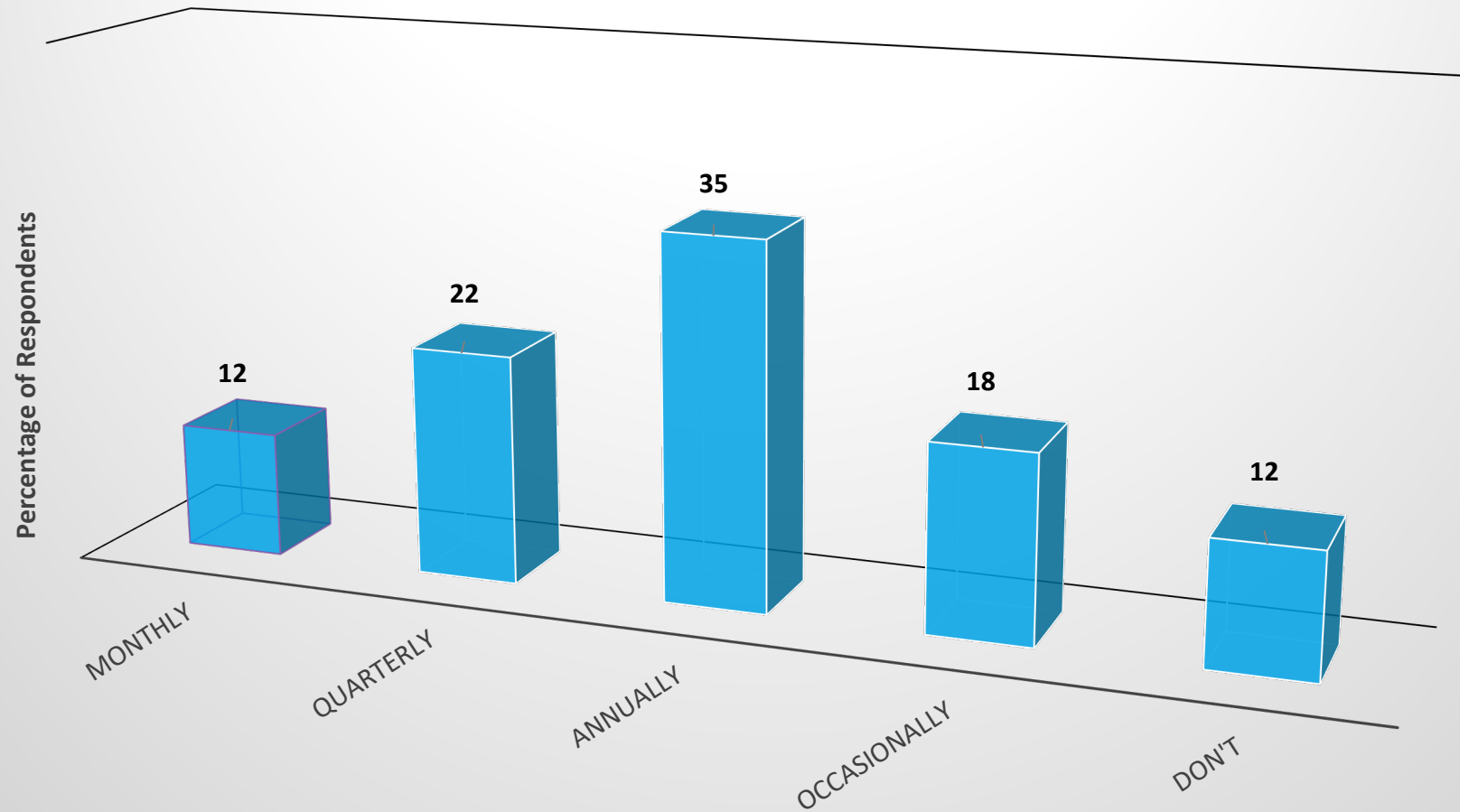


In the U.S., the greatest concerns are cloud account compromise (**39%**), followed by supply chain attacks (**38%**), and insider threats and cyber/physical attacks (both **37%**).

Managing Risk in the Cloud vs. Traditional IT



How often do you manage your risk management metrics?



How Enterprises Manage Risk in the Cloud

Less than half (48%) continuously evaluate the risk status of cloud services used after procurement.

CSA's [*The 12 Most Critical Risks for Serverless Applications*](#)

[HTTPS://CLOUDSECURITYALLIANCE.ORG/](https://cloudsecurityalliance.org/)

Annual CSA Top Threats Report

*Early data shows that these threats, risks & vulnerabilities currently are rated highest (listed in alphabetical order).

Accidental Cloud Data Disclosure

Cloud Storage Data Exfiltration

Data loss, Destruction or Tampering

Insecure Interfaces and APIs

Insufficient Identity, Credentials Access & Key
Management, Privileged Accounts

Lack of Cloud Security Architecture & Strategy

Organized Crime/Hackers/APT

**Subject to change as these are very early results for research report to be released in February 2022.*

Other Worries Plaguing Journeys to the Cloud

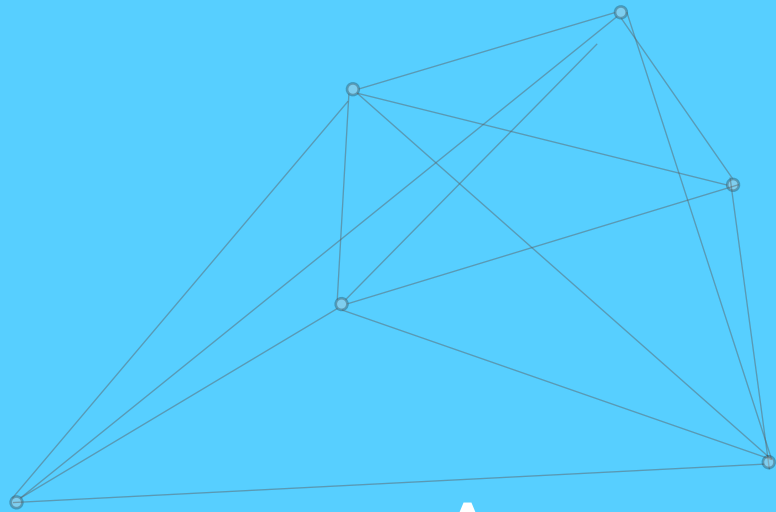
Concerns when running applications in public cloud



- 1** Clear visibility (topology, policy) for the entire hybrid network estate (multi-cloud and on-prem)
- 2** Proactively detect network risks
- 3** Proactively detect misconfiguration risks (e.g. IAM)
- 4** Automation, uniform change management across the different security controls
- 5** Regulatory compliance reports
- 6** Clean up cloud security controls with excessive rules
- 7** Ease of migration of workloads from on-prem to cloud

Respondents were also asked about their concerns once applications were running in the public cloud.

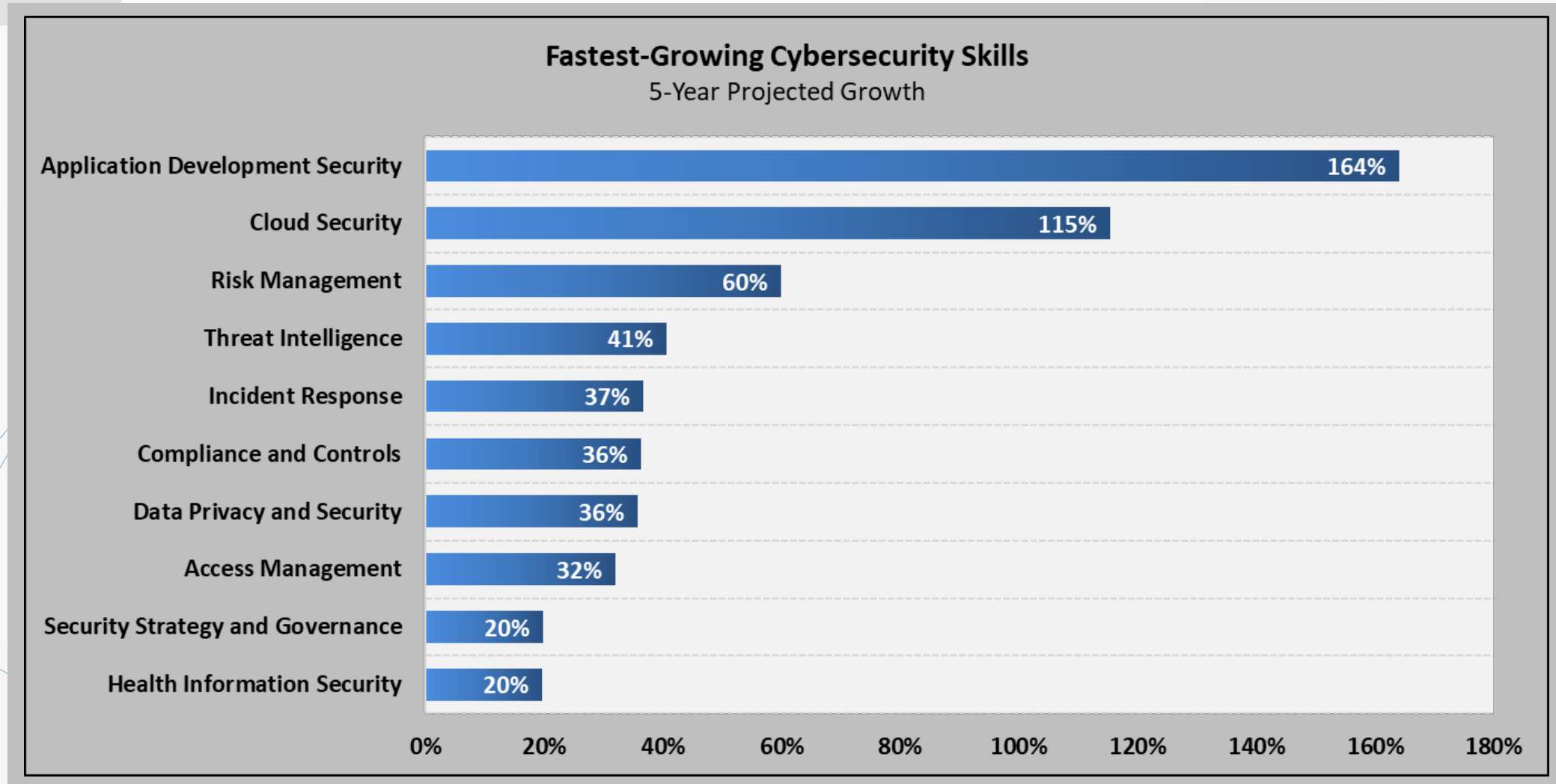
On average, the highest ranked security concern was "sensitive data leakage," which is consistent with the previous survey in 2019. "Services outages", "configuration and security settings", "unauthorized internal access", "compliance with regulatory compliance", and "ransomware" received a similar average ranking of about moderate concern. Although "vendor technology vulnerabilities" received the lowest average ranking, it fell just below moderate concern. This was somewhat surprising since the SolarWinds hack was reported while this survey was open. However, even with this issue being more salient, it still was the lowest ranked issue.



2021:
Approximately 3.5 million
cybersecurity job
openings

Source: Global Research Firm Cybersecurity Ventures

Wanted: Cloud Security Knowledge



Burningglass Technologies, a labor market analytics firm, analyzed its database of over 1 billion historical job records & projected five-year growth rates for skills across the cybersecurity space to help organizations, training providers & individuals understand the knowledge needed to prepare for the future.

Up-leveling Skill Sets for Cloud

Addressing the skills gap in cloud security

The top three ways organizations are addressing the skills gap are "industry training and certifications for staff" (55%), "informal or staff self training" (54%), and "customer training from vendors on products" (53%). Much less commonly selected at 27% was outsourcing staff. The least frequently selected option was "not addressed" at 7%.

Industry trainings and certifications for staff
(e.g. CSA, ISC2, ISACA, SANS)

55%

Informal or staff self training

54%

Customer training from vendors on products

53%

Outsourcing staff

27%

Not addressed

7%

Unsure

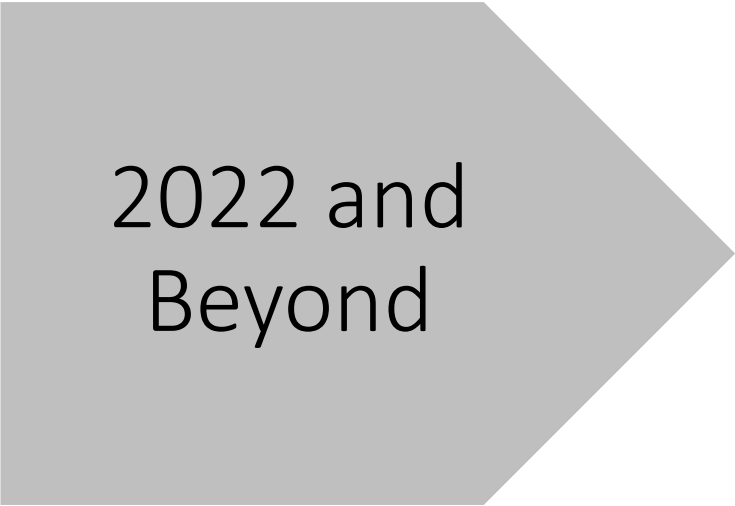

5%

Other (please specify)

2%

[State of Cloud Security Concerns, Challenges, and Incidents](https://cloudsecurityalliance.org/). CSA (2021)

[HTTPS://CLOUDSECURITYALLIANCE.ORG/](https://cloudsecurityalliance.org/)



2022 and Beyond

“The global pandemic has necessitated a re-evaluation of security programs across many industries and mandate changes in policies and technologies. The network edge has become a fluid entity that follow every remote worker. As security professionals, we have to remain nimble to respond to the evolving attack survey, dynamic ransomware and evolving insider threats.”

Martin Littman, CTO & CISO,
Kelsey-Seybold Clinic

CSA's CxO Trust

Seeking a common understanding & knowledge of cloud computing, as well as help progress solutions & standards to meet the cybersecurity challenges confronting all C-level stakeholders, their executive teams & governing bodies.



CSA's CxO Trust



Trusted Community

Collective Voice

Power of Influence





1st year in InfoSec



3 years in InfoSec

The Build

- Broad-based Program in Phases
- Community - CISOs & other C-Levels
- Research, Guidance, Use Cases...
- Hands-On Training, Discussion Groups, Roundtables, & More
- Add-ons to current offerings
- Other benefits - Chapters/Members
- Expertise Building, Mentoring, Hiring Help – Beyond Job Boards

CxO Trust Advisory Council

- Contributes to/advises on overall strategy, roadmap & related offerings
- Helps guide our CxO Trust Research Working Group
- Composed of CISOs, Chief Information/Chief Technology Officers, Chief Risk Officers, Chief Privacy Officers, Chief Compliance Officers, Chief Operating Officers, Chief Executive Officers & other C-level stakeholders
- Reserved for the participation of C-level executives from CSA Corporate Members



CxO Trust Advisory Council

- Mike Anderson, Chief Digital & Information Officer, Netskope
- Raj Badhwar, CISO, Voya Financial
- Rolf Becker, Co-Founder & Chair, European User Group Enterprise & Cloud Data Protection (EuUG)
- Rachel Bierner, SVP, Cloud Security Leader, Wells Fargo
- Fred Budd, VP, Cloud Security, Mastercard
- James Cairns, Security Lead, Bow Valley College
- Peter Campbell, Director, Security Engineering, Cigna Technology
- Ben Carr, CISO, Qualys
- Sean Catlett, CSO, Slack
- Dave Cullinane, Founder, TruStar Technology (now part of Splunk)
- Jim De Haas, Secretary, ABN AMRO Global Cloud Governance Board
- Stacey Halota, VP, Information Security & Privacy, Graham Holdings
- Jason Johnson, Lead Information Security Assessor (VP), Citi
- Suyesh Karki, CISO, Domo



CxO Trust Advisory Council

- Anil Karmel, Co-Founder & CEO, C2 Labs
- Andy Kirkland, Global CISO & VP, Global Cybersecurity Services, Starbucks
- Ricardo Lafosse, CISO, Kraft Heinz
- V. Jay Larossa, Head of Global Trust Assurance, TikTok
- Adrian Ludwig, Chief Trust Officer, Atlassian
- Shehzad Merchant, Chief Technology Officer, Gigamon
- Aaron Miller, CISO, New York State Office of the Attorney General
- Gerald Parham, Global Research Leader, Security & CIO, IBM Institute for Business Value
- Vinay Patel, CISO, Finastra
- Edgar Pimenta, VP, Information Security, TalkDesk
- Mindy Player, Director of Cloud Security, Lloyds Banking Group
- Janice Reese, CEO, Network PDF Cloud Solutions
- Marisa Ruffalo, Cybersecurity R & D Specialist & Distinguished Engineer, Chevron
- Joe Zacharias, Deputy CISO for Cybersecurity Risk Management, Caterpillar

CxO Trust Research Working Group

- Creates all CxO Trust-related research & other informational assets
- Provides additional input/ideas on other relevant offerings
- Open to industry pros who are interested in actively contributing to this initiative (participants do not have to be employees of CSA Corporate Members)
- Already have confirmed some 80 members
- CSA Research to get in touch in next week to share proposed research calendar for comment & set first meet for January 2022

Some Topics Discussed in Kick-Off *

Moves from
On-Prem Systems
to Cloud

Cross-Cloud-
Platform Security
Strategy

Architecting Multi-
Cloud Environments
leveraging a Zero
Trust model

Security Operations
& Response

Establishing a
“Wellness Program”
for Cloud
Environments

Making Digital
Transformations
Business Enablers

Regulatory
Compliance in the
Cloud

Finding Cloud
Expertise

Cloud/SaaS Supply
Chain Security

**Subject to change.*

CSA Resources

- [Security Guidance for Critical Areas of Focus in Cloud Computing](#)
- [Cloud Controls Matrix \(CCM\)](#) – Assess your compliance to cloud standards.
- [Consensus Assessment Initiative Questionnaire \(CAIQ\)](#) - Security questionnaire for vendors.
- [Top Threats to Cloud Computing](#)
- [Enterprise Architecture](#)
- [Cloud Threat Modeling](#)
- [Secure Connection Requirements of Hybrid Cloud](#)
- [Hybrid Cloud and its Associated Risks](#)
- [Top 10 Blockchain Attacks, Vulnerabilities & Weaknesses](#)
- [State of Cloud Security Risk, Compliance & Misconfiguration](#)
- [State of Cloud Security Concerns, Challenges & Incidents](#)

Cloud Threat Modeling



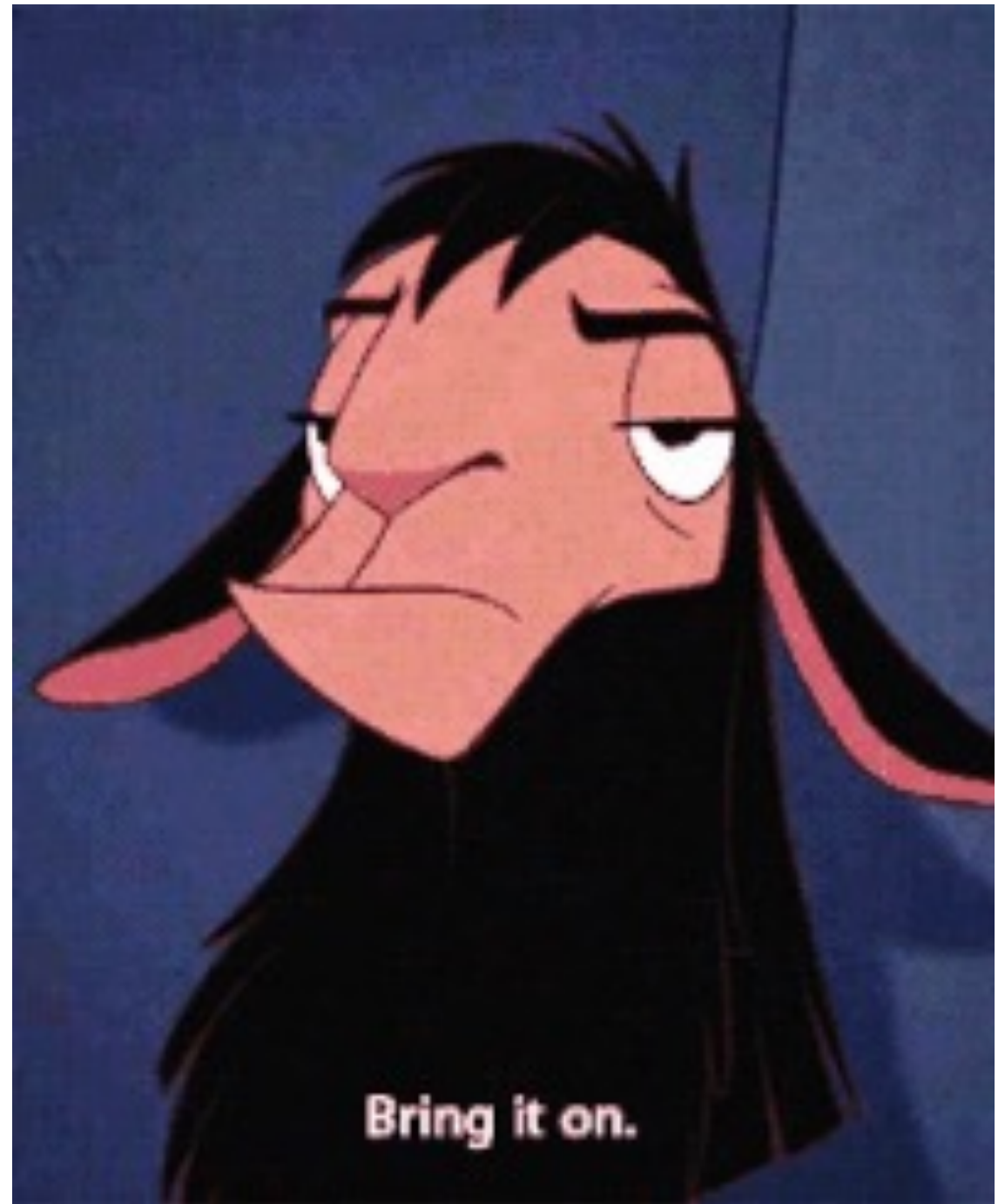
Key Takeaways:

- The baseline threat modeling processes taken from various standards and best practices
- The differences between standard threat modeling and cloud threat modeling
- How to create a cloud threat model from scratch
- A basic cloud threat model reference
- What should be included in a detailed security design report
- Example cloud threat modeling cards

CSA Resources & Ways to Engage with Us

- [CSA STAR Registry](#) – Security, Trust, Assurance & Risk Registry to find providers with the right level of security and data privacy for your organization.
- [CSA Education](#) – Training, certificates (Certificate and Cloud Security Knowledge & Certificate of Cloud Auditing Knowledge) & more educational resources
- Membership - [Join CSA as a business](#) or [participate as individual in relevant Chapters](#).
- [Network – Join Circle](#), CSA's online community forum platform to connect with peers.
- [Research Working Groups](#) – Explore & consider joining a research working group.

And 2022...





Illena Armstrong,
Cloud Security Alliance President

Contact details for Illena

Cloud Security Alliance:
iarmstrong@cloudsecurityalliance.org

LinkedIn:
<https://www.linkedin.com/in/illenaarmstrong/>

Twitter: @illena_a