



2024 LIFE
INSURANCE
& ANNUITY
CONFERENCE

**Powering
Growth**

Countering (or Overcoming) the Evolution of Insider Threats Among the Changing Workplace Landscape





Jamie Wong

Senior Director, Internal Investigations
Nationwide



Sandra Desautels

Partner, Financial Crimes, Fraud & Investigations
Guidehouse

Insider Threats are Increasing - What is Your Plan?

With the predominant virtual workplace environment, and growing use of third-parties to support your operations, insider threats may be greater than you realize.

Defining Insider Threats

Risk posed by vulnerabilities in key systems or by individuals in an organization who misuse their access, knowledge, or authority to intentionally or unintentionally harm the company.

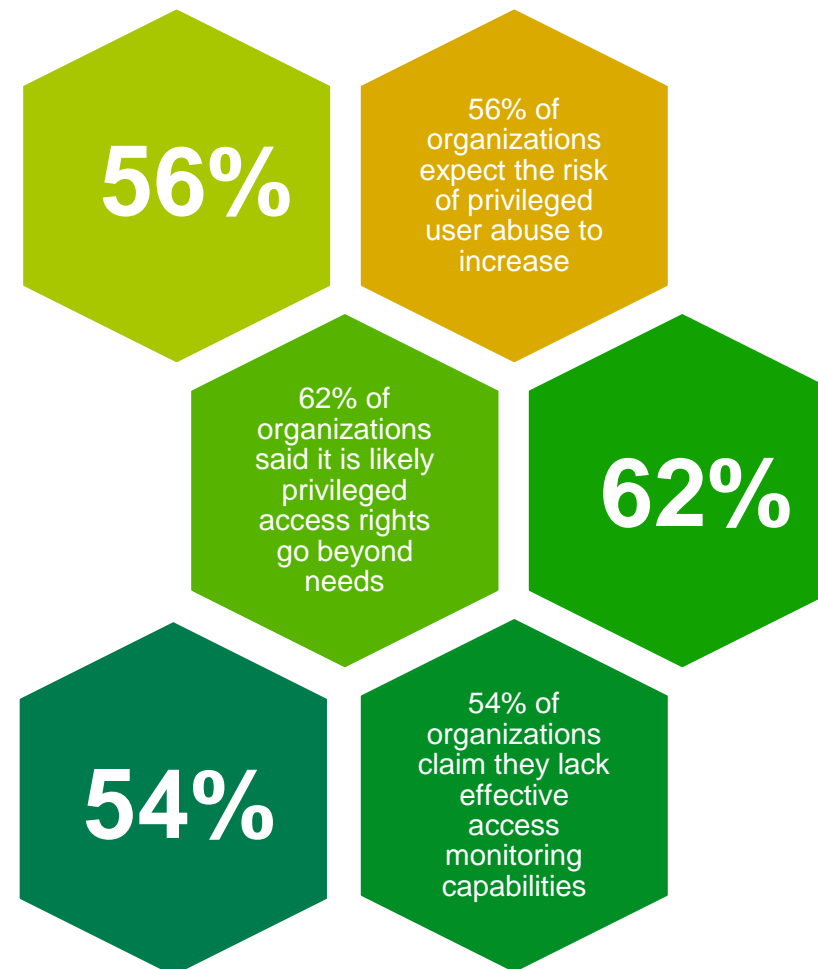
1

Employee or member of an organization



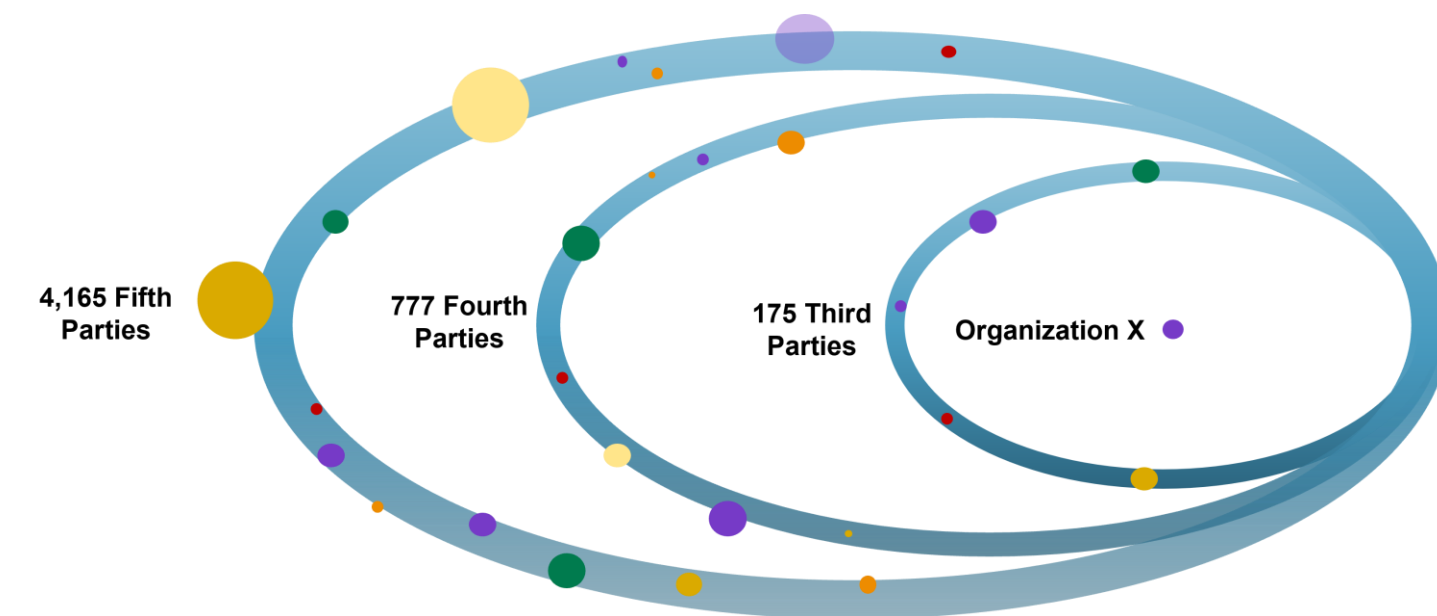
2

Privileged Users and Administrators



3

Third Parties and Nth parties



Defining Insider Threats

The landscape of insider threats is diverse, encompassing employee fraud, occupational fraud, data and financial breaches because of various forms of intent



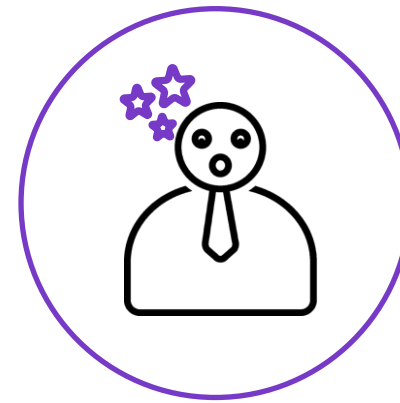
Malicious Insiders

An employee or contractor with authorized access intentionally misuses or steals sensitive information for personal gain or to harm the organization.



Agnostic Fraud

Fraud that is not motivated by malicious feelings towards the company itself, but purely by opportunity for personal gain.



Naive Insiders

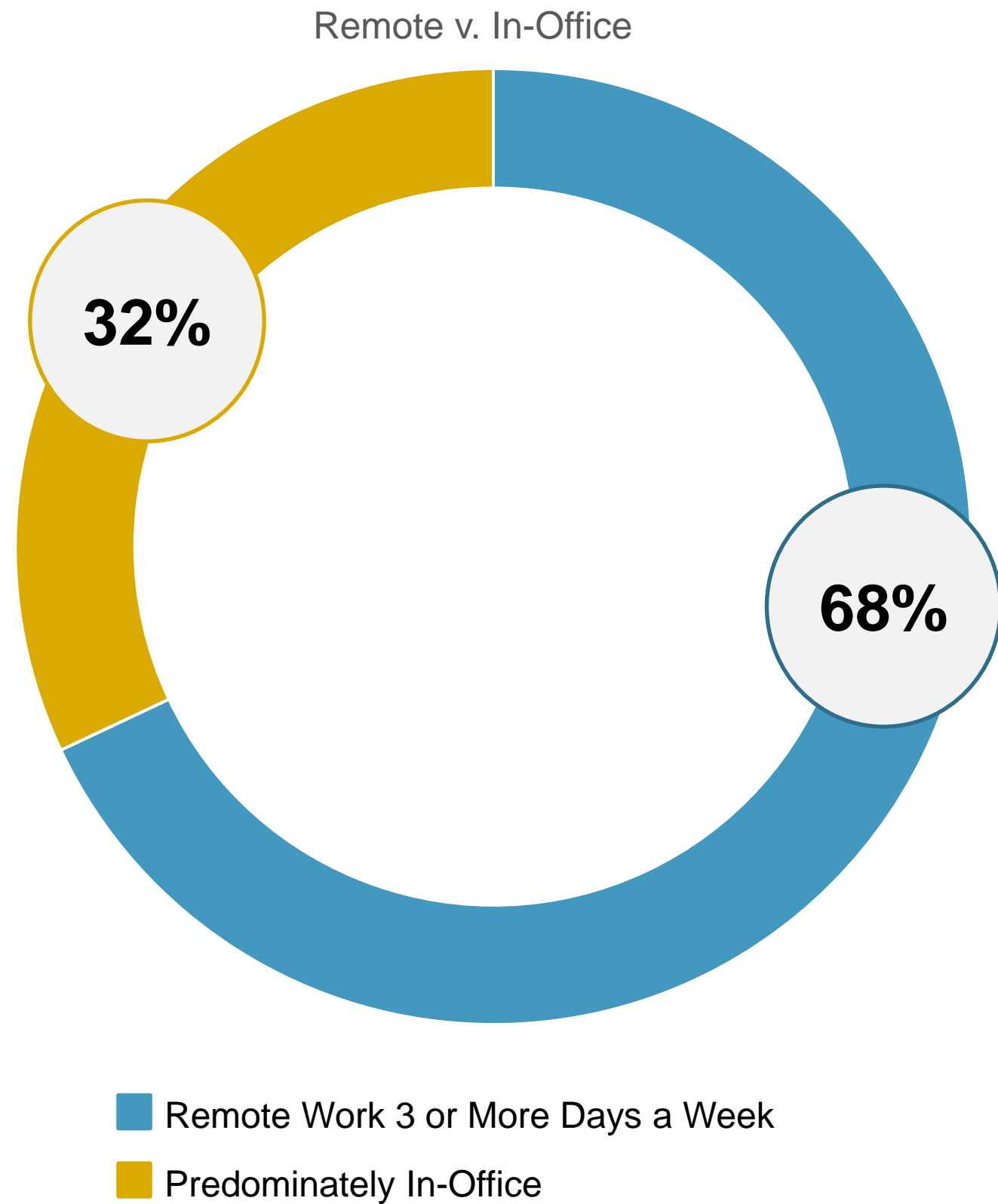
An employee or contractor becomes unknowingly complicit in fraud through being targeted by external fraudsters.



Negligent and Careless Insider Fraud

Insiders inadvertently expose sensitive data due to a lack of training, negligence, or carelessness.

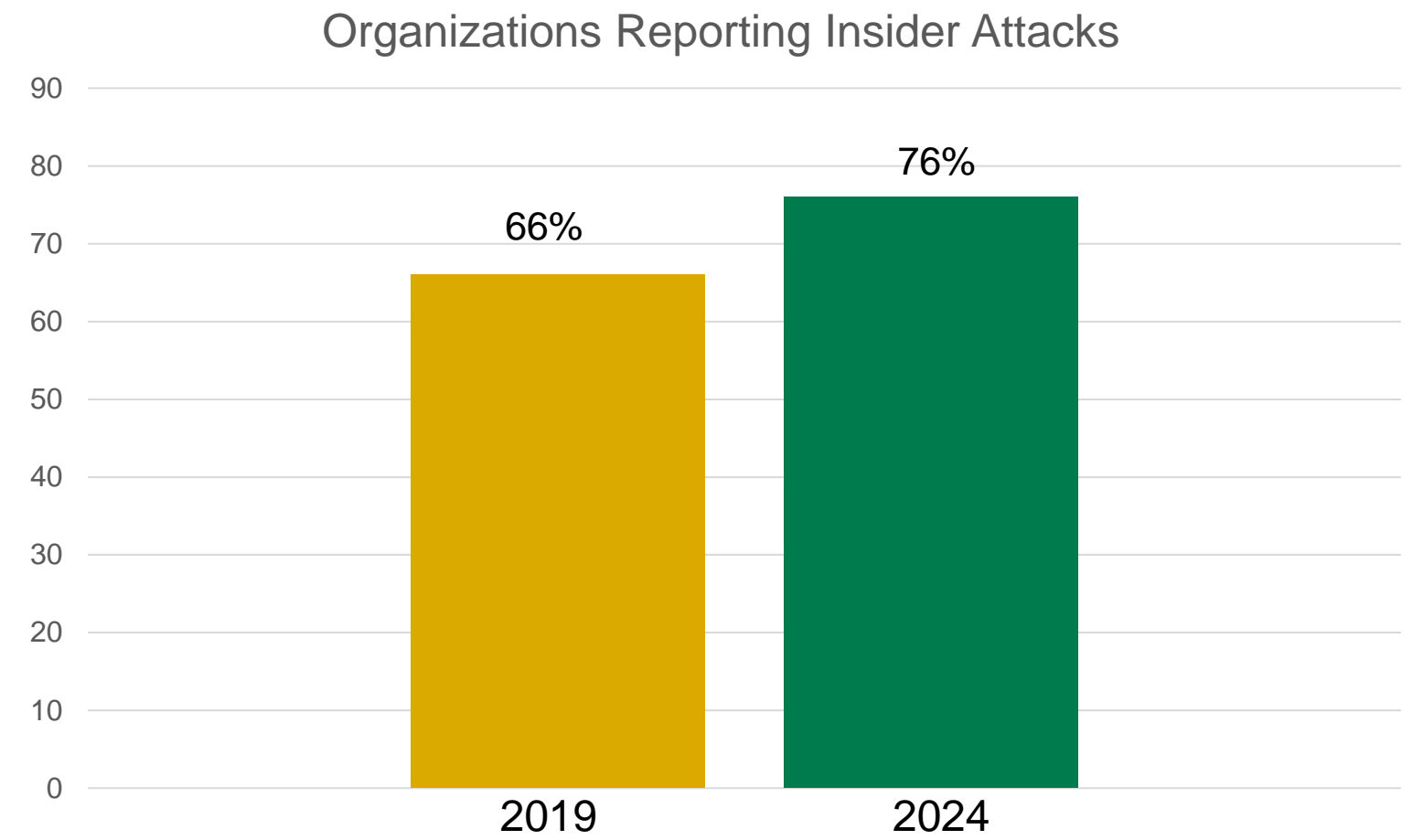
The Changing Environment



Source: Insurance Information Institute

70%

70% of cybersecurity professionals have expressed concerns of insider threats in hybrid work environments



Source: Cybersecurity Insiders





Safeguarding Data



Poll Question

Are you concerned
about the potential
misuse or
exploitation of data
in your
organization?

Data Preservation and Protection



Data Sharing



Data Usage



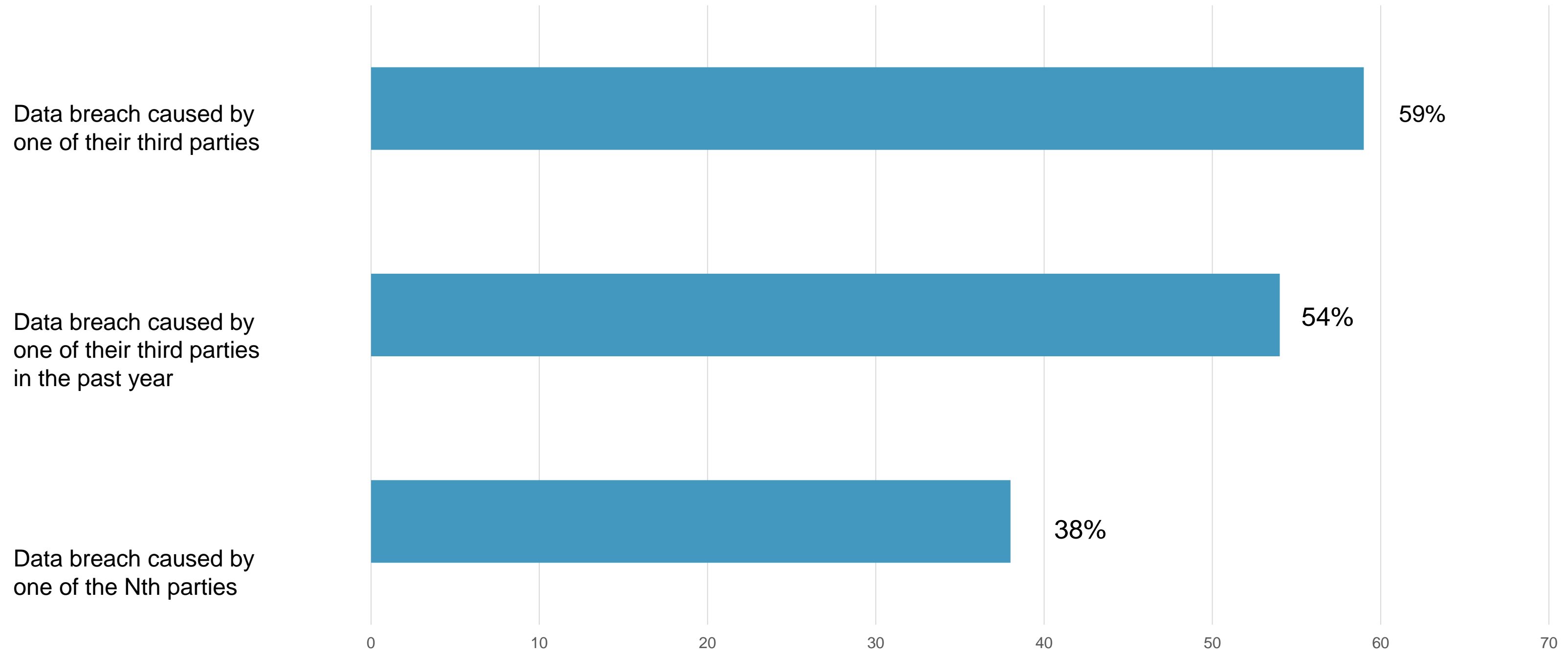
System Controls



Manual Controls

Third Party Risk

Organizations That Experienced a Data Breach Caused By a Third Party



Source: Ponemon Institute





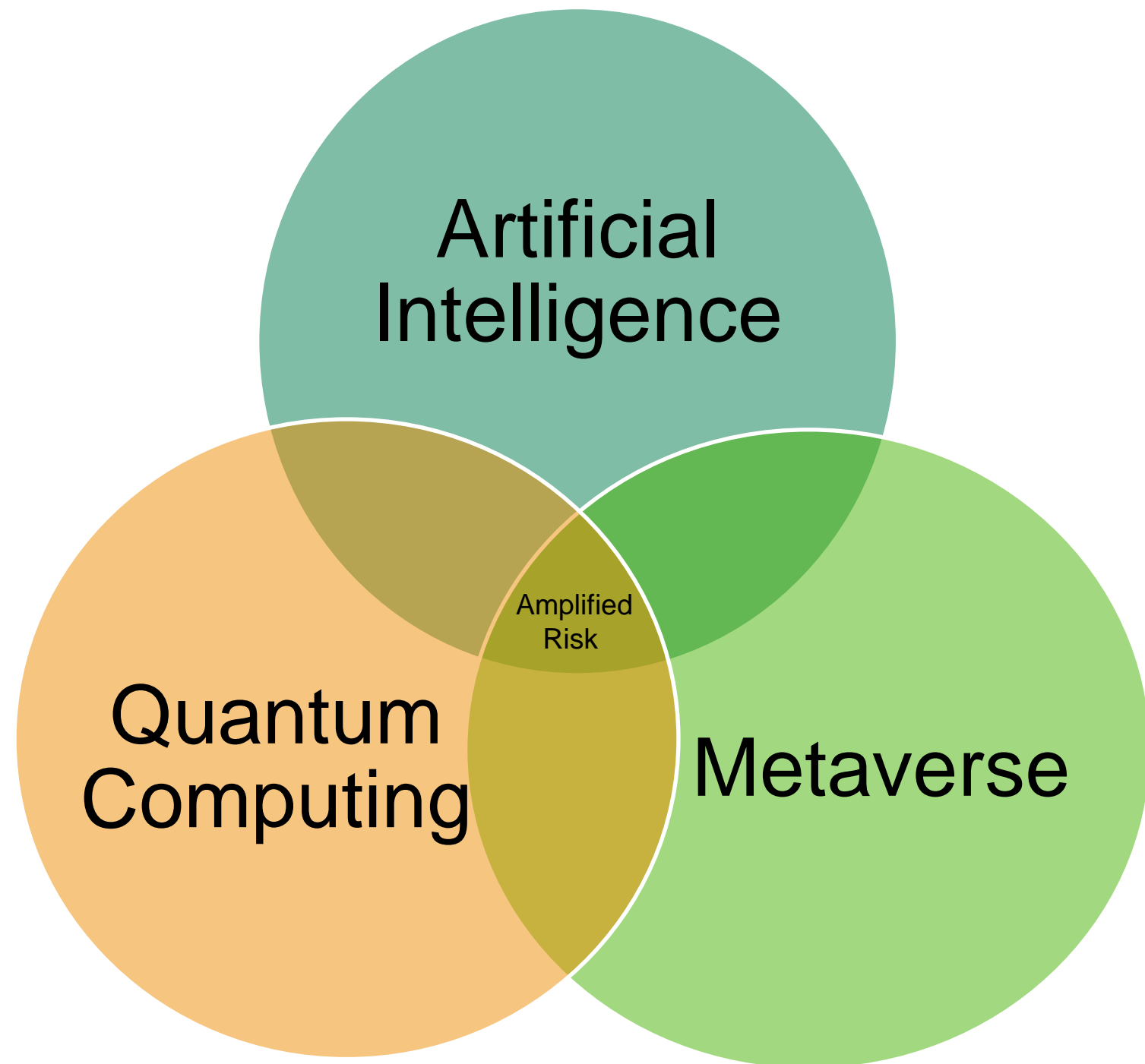
Top Industry Trends



Poll Question

Do you have a
clear
understanding of
how your
organization is
structured to
combat insider
threats?

The Changing Environment



AI

$\frac{3}{4}$ of cybersecurity professionals are concerned with the impact of new technologies on insider threats.

90%

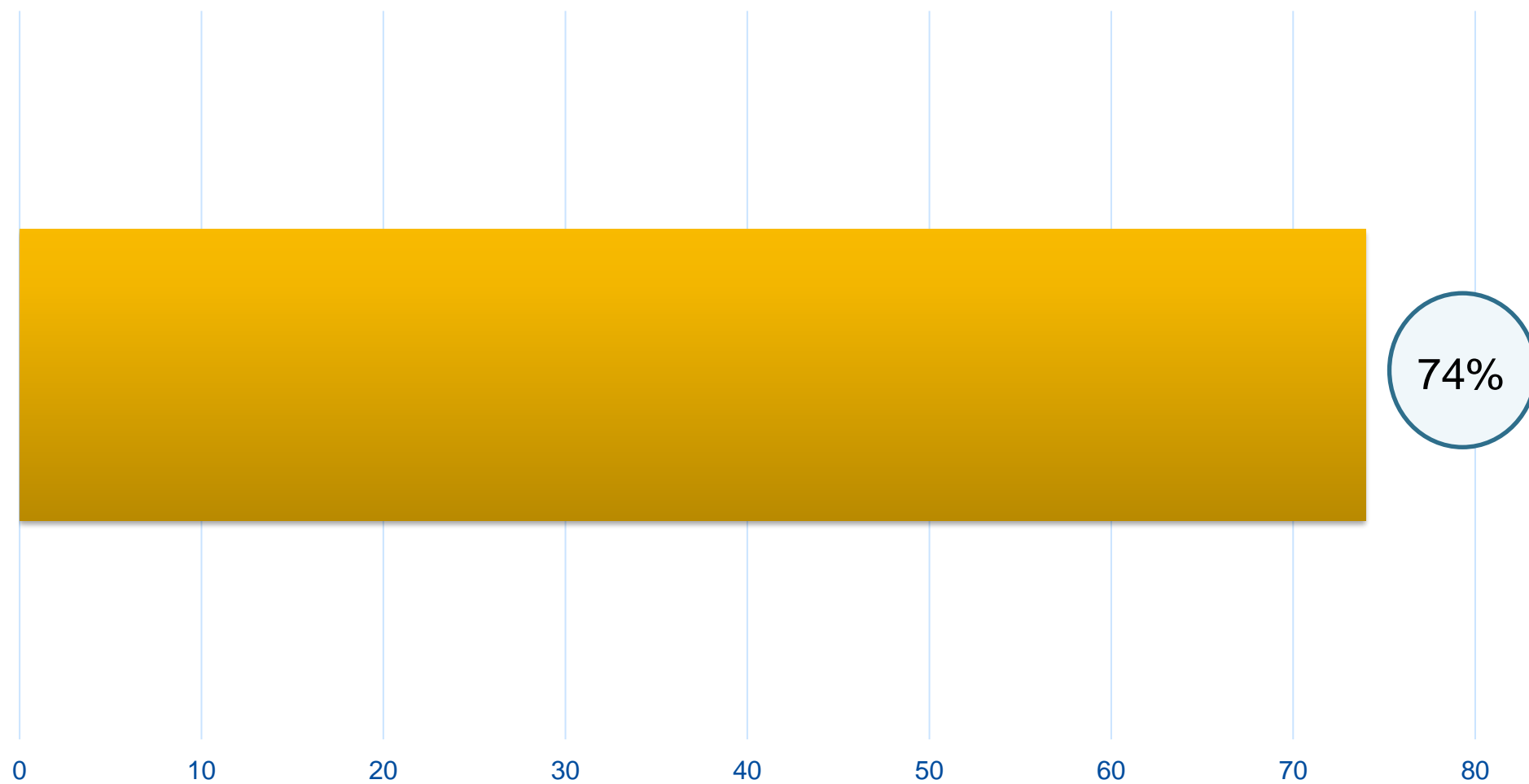
90% of cybersecurity professionals report insider attacks are equally or more challenging to detect than external

Source: Cybersecurity Insiders



The Changing Environment

2023 Data Breaches That Involved Human Element



Social Engineering

Privilege Misuse

Stolen Credentials

Error

Business Email Compromise (BEC) attacks have nearly doubled in the last 5 years.

Now BEC represents over 50% of Social Engineering Incidents



Source: Verizon



**2023 Insider
threats
informing 2024
priorities**

Third party risk management

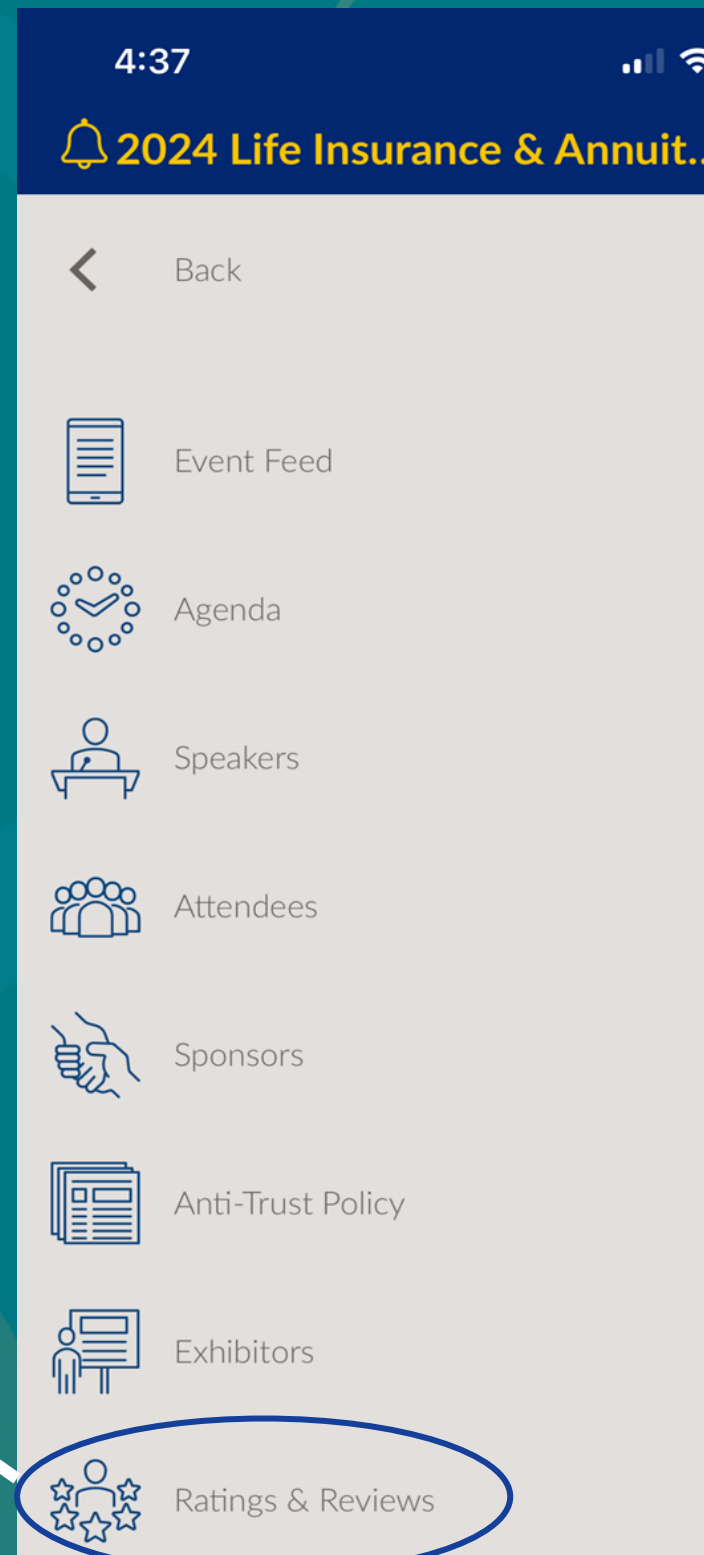
Data loss prevention

Virtual hiring & monitoring

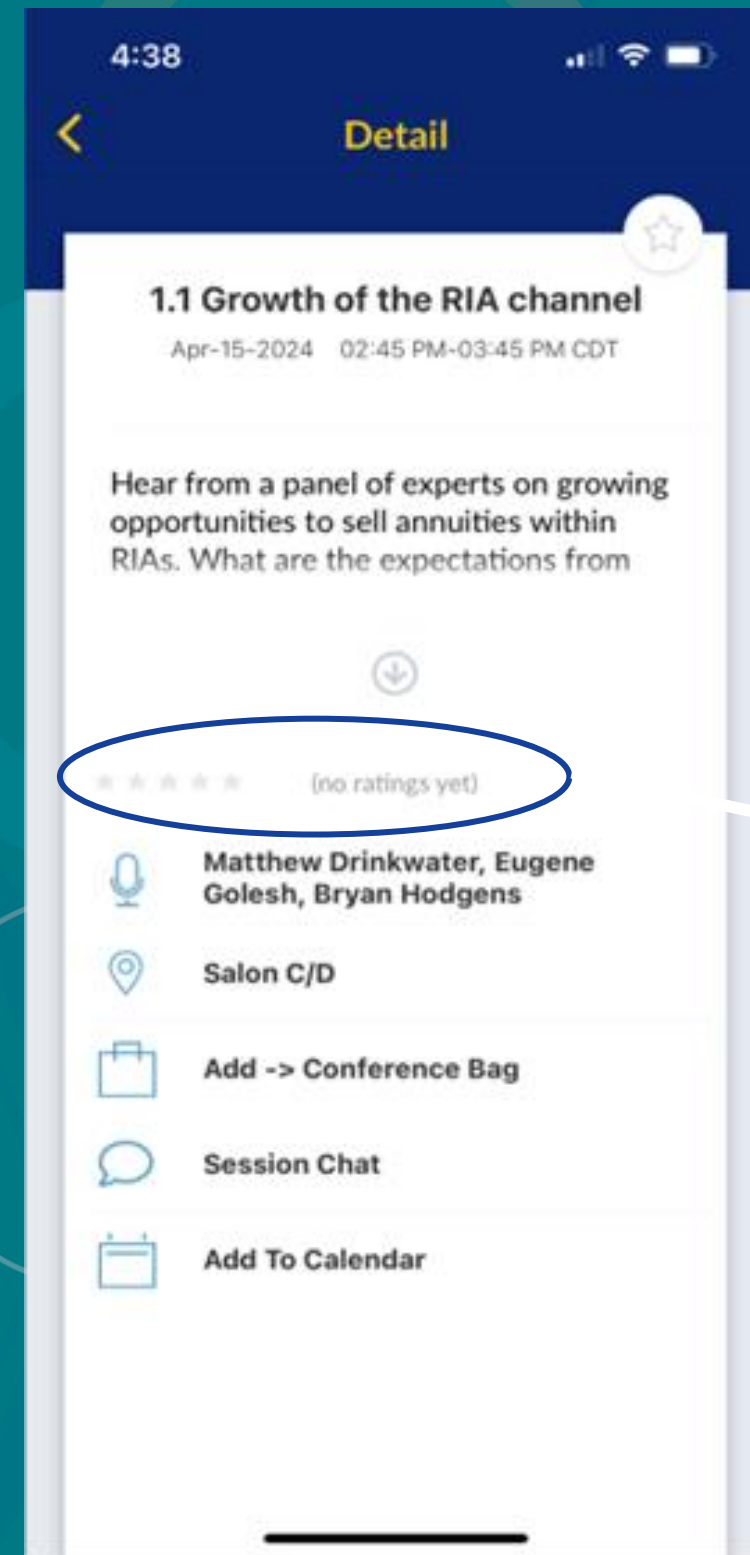
Access management

Please Provide Your Feedback on the Conference App

OPTION 1



OPTION 2



Thank You

