Cyber Crime

—

Ashely Singh

Agenda

—

◈ A real-world example

◈ Cyber Extortion in South Africa and Globally

◈ Detection Threats and Incidents

◈ What Sanlam does and what you can do

Real World Example

—

about Ashley Singh

- ◈ ID Number
- ◈ Tax Number
- ◈ Home Address + what seems to be previous properties owned
- ◈ Where he runs
- ◈ Email addresses (work + Personal)
- ◈ Cellphone number
- ◈ Articles he appears in
- ◈ Family Details: (Children's Names + Where they go to School)
- ◈ Details on his wife (Name + ID + Tax Number + Cell Number + Addresses tied to her)
- ◈ Siblings and Cousins names/social profiles
- ◈ Last International Holiday
- ◈ Breached credentials for his wife
- ◈ His secret desire to become an accountant (NOT true if you've read this far)
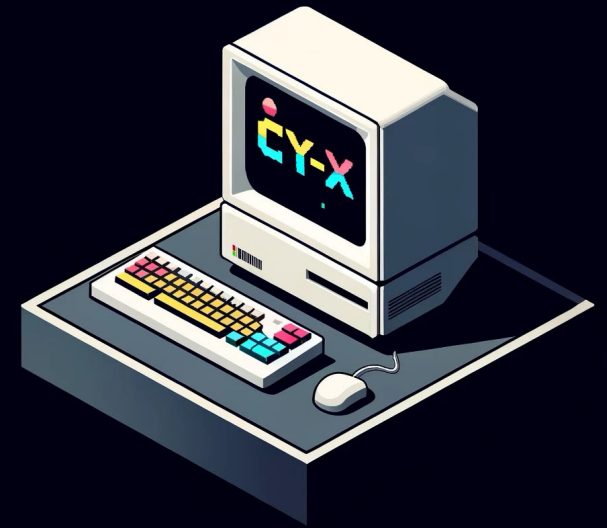
CYBER EXTORTION
CY-X
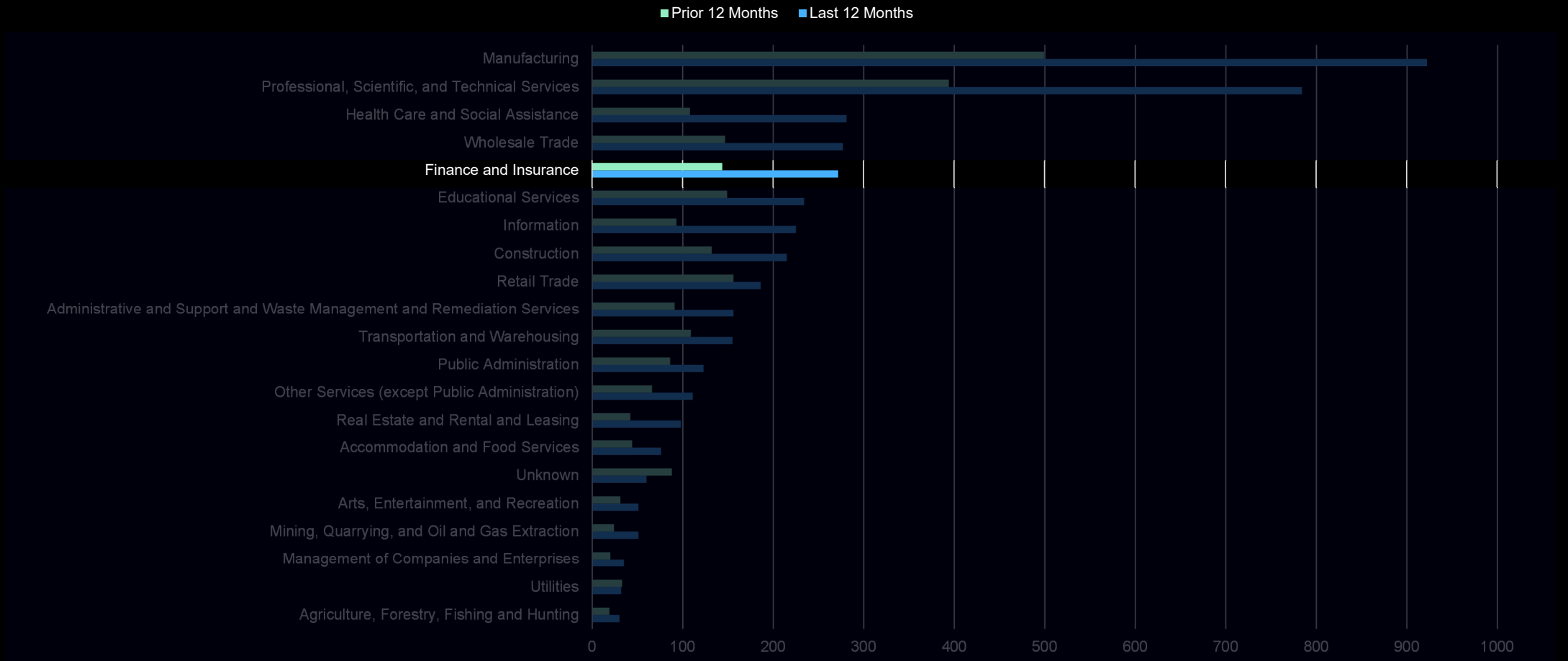
 from our dark net surveillance
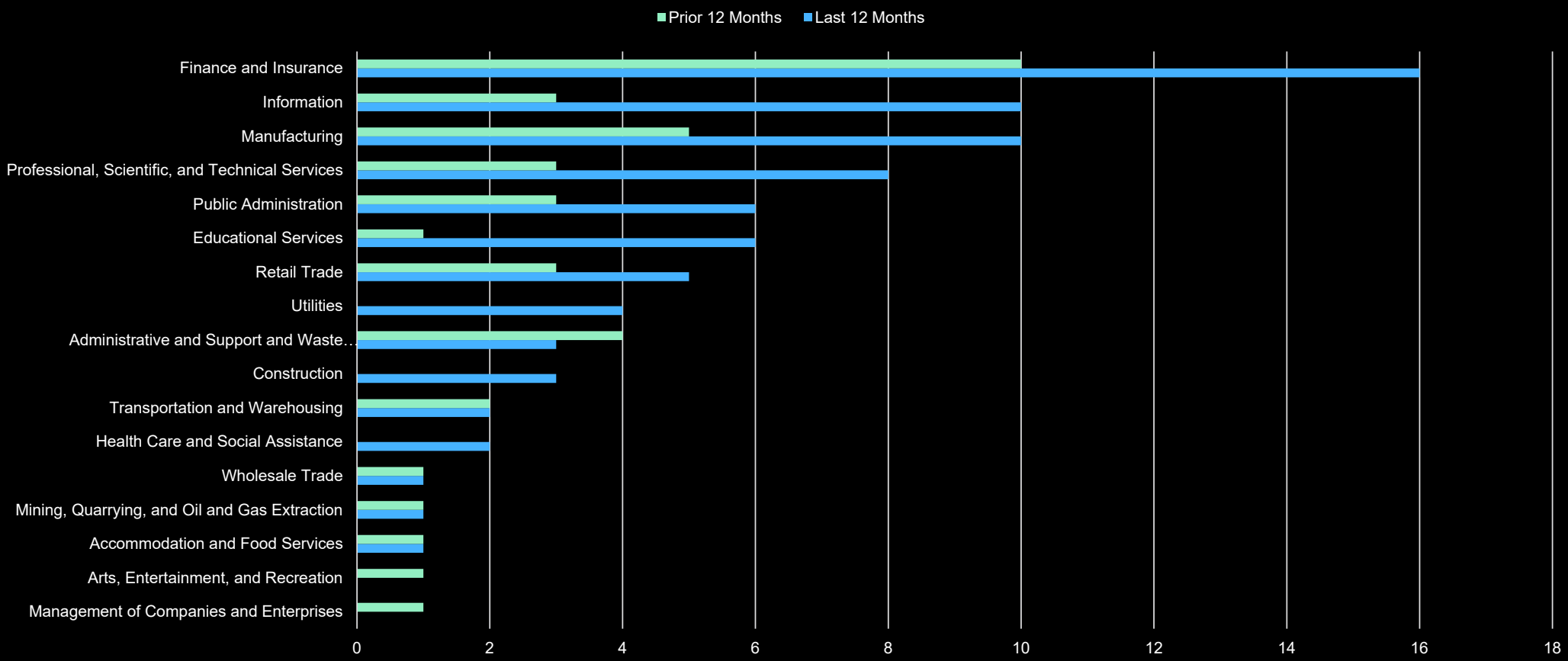
C:_

Cy-X over time

**Victims and actors count observed on double-extortion leak sites over time**

Shift in victims by industry – Globally | Industry breakdown:
Comparison between the last and prior year (April 2022 – March 2024)
—

Shift in victims by industry – Africa | Industry breakdown:
Comparison between the last and prior year (April 2022 – March 2024)
—

Legend: ■ Prior 12 Months ■ Last 12 Months

Industry	Prior 12 Months	Last 12 Months
Finance and Insurance	10	16
Information	3	10
Manufacturing	5	10
Professional, Scientific, and Technical Services	3	8
Public Administration	3	6
Educational Services	1	6
Retail Trade	3	5
Utilities		4
Administrative and Support and Waste…	4	3
Construction		3
Transportation and Warehousing	2	2
Health Care and Social Assistance		2
Wholesale Trade	1	1
Mining, Quarrying, and Oil and Gas Extraction		1
Accommodation and Food Services	1	1
Arts, Entertainment, and Recreation	1	
Management of Companies and Enterprises	1	

Shift in victims by industry – South Africa | Industry breakdown: **Comparison between the last and prior year** (April 2022 – March 2024)
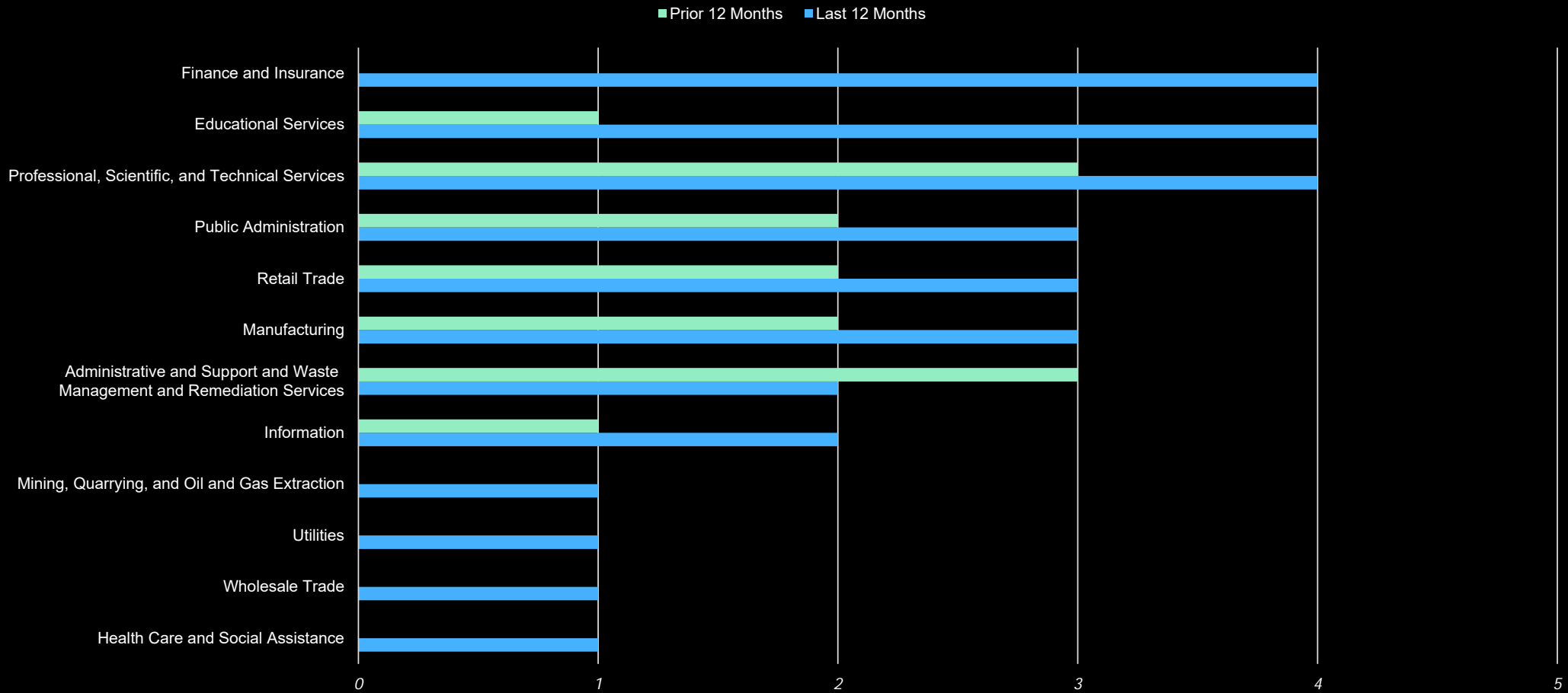
Threat Detection:
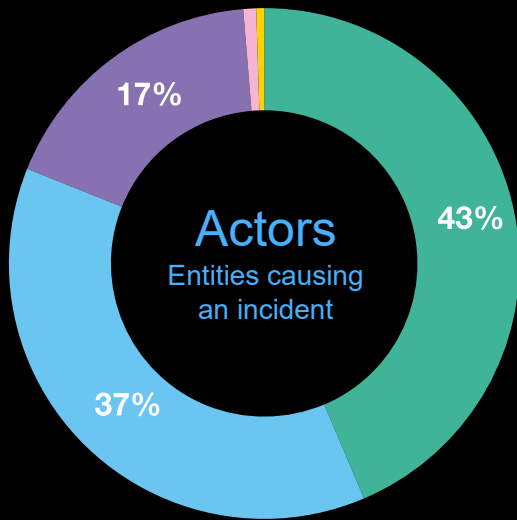**Statistics from our CyberSOC threat hunting operations**
—

Number of incidents
## CyberSOC data analyzed (October 2022 to September 2023)
—

129,395 Potential incidents ▶ **25,076** Confirmed incidents **(=19.37%)**

Actors
Entities causing an incident

- 43%
- 37%
- 17%

Legend:
- External
- Internal
- Unknown Actor
- Other
- Partner

Action
What the threat actor(s) did

- 30%
- 17%
- 14%
- 13%
- 7%
- 7%
- 6%
- 3%

Legend:
- Hacking
- Misuse
- N/A
- Malware
- Error
- Social
- Other Action
- Physical
- Environmental

Asset
The asset that was affected
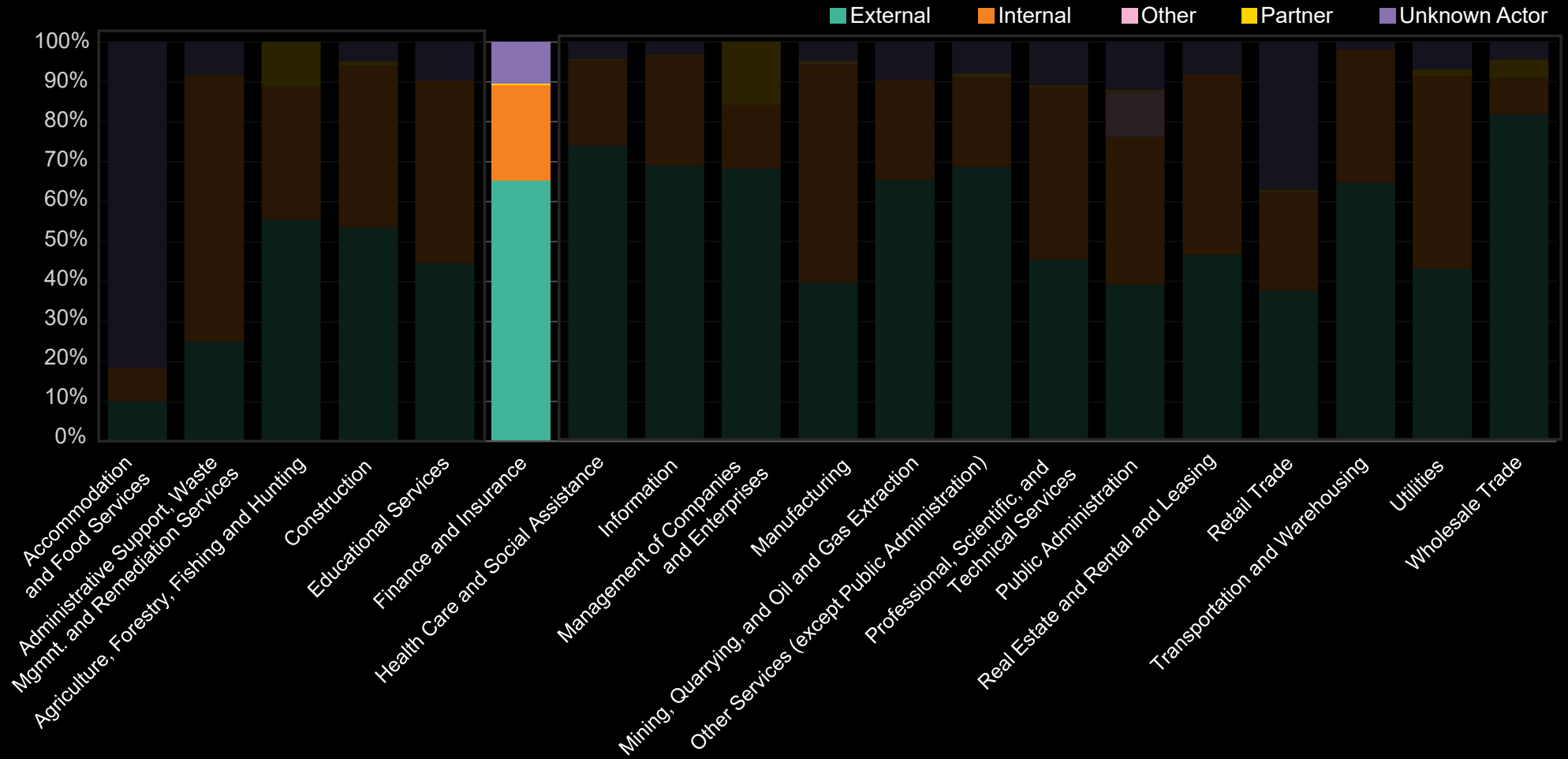
- 28%
- 27%
- 19%
- 7%
- 6%
- 5%
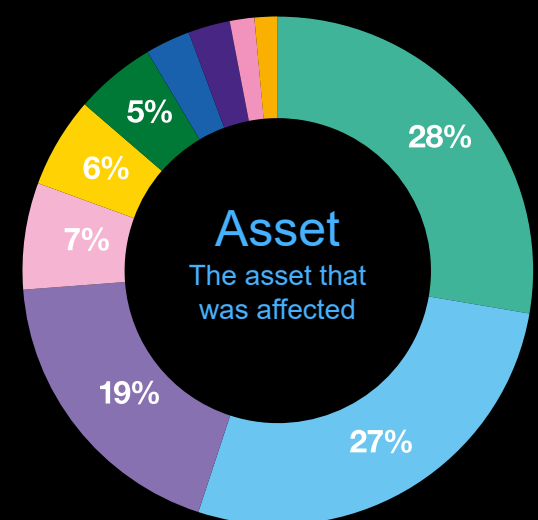
Legend:
- End user device
- Server
- Unknown Asset
- Account
- Network
- Multiple
- Other
- People
- Media
- Cloud

Sources of incidents by industries
Breakdown of confirmed incidents by actor and vertical

—

Legend: External, Internal, Other, Partner, Unknown Actor

Categories: Accommodation and Food Services; Administrative Support, Waste Mgmnt. and Remediation Services; Agriculture, Forestry, Fishing and Hunting; Construction; Educational Services; Finance and Insurance; Health Care and Social Assistance; Information; Management of Companies and Enterprises; Manufacturing; Mining, Quarrying, and Oil and Gas Extraction; Other Services (except Public Administration); Professional, Scientific, and Technical Services; Public Administration; Real Estate and Rental and Leasing; Retail Trade; Transportation and Warehousing; Utilities; Wholesale Trade

Administrators' ability
to mitigate Cybercrime
—

Survey of 184 Employer and Umbrella Funds.

7/10 expressed concern around Cybersec especially with 2 pot enactment.

Despite this, 4/10 Umbrella Fund participants assess SP Cyber Risk readiness.

Administrators provide us with a copy of their cyber security policy
- 64%
- 28%

We conduct due diligence at the administrator's office
- 44%
- 21%

Include questions in the tender document which deal with cyber security
- 27%
- 9%

We have a standard checklist which they must complete
- 24%
- 13%

Currently do not evaluate this as part of the tender process, but on the agenda for future implementation
- 1%
- 9%

Not part of our assessment process
- 5%
- 39%
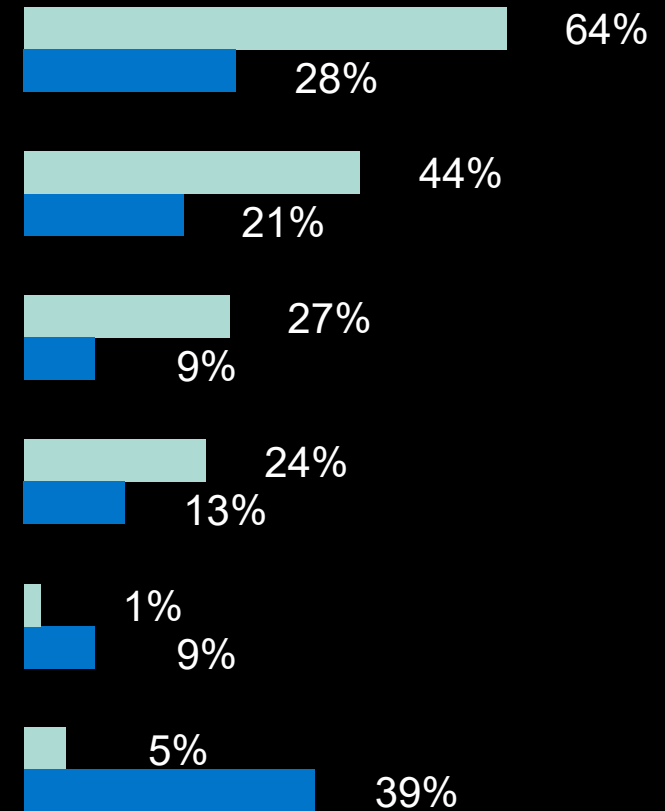
What can you do and
what is Sanlam doing?

—

What is Sanlam doing?

—

What can I do?

—

Stay proactive both in your personal capacity and in the workplace.

⊗ Report incidents.

⊗ Monitor your bank account.

⊗ Make all your accounts online private.

⊗ Use strong passwords or pass phrases.

⊗ Change your passwords.

⊗ Use 2 factor authentication.

⊗ Scan your pc for malware regularly.

⊗ Monitor your calls and emails for suspicious contacts.