MISA Ontario

2024 Municipal Cybersecurity Outlook Survey Report

MISA Ontario

Advancing Digital Transformation

Municipal Information Systems Association, Ontario

MISA Ontario

Who are we?

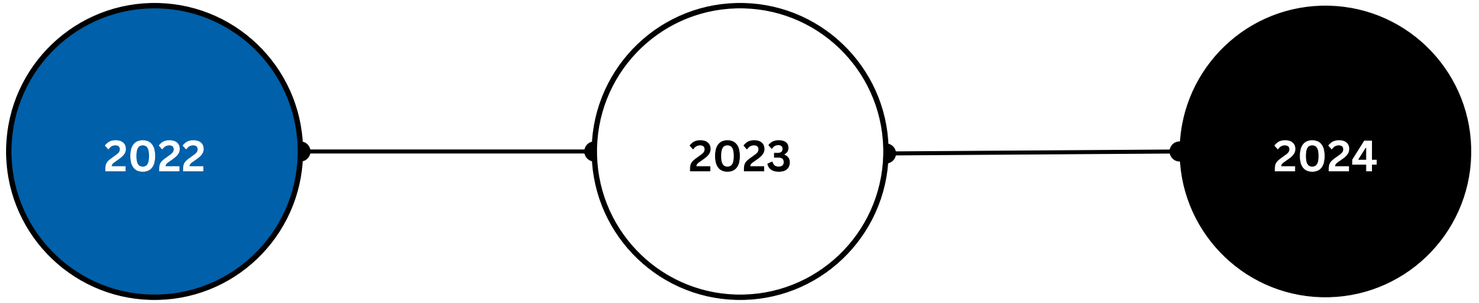
- Non-profit organization providing a centralized hub for municipalities
- A community of experts & practitioners providing leadership, guidance, and resources for anyone interested in using technology to improve municipal services.
- Represent 1400+ dedicated professionals working towards a more effective government

The Association's services are built around three core areas:

- Networks and Communities
- Events and Professional Development
- Shared Knowledge

2024 Cybersecurity Outlook Survey

Overview



- **Initial launch** of cybersecurity outlook survey
- **64** municipalities

- **75** municipalities

- **86** municipalities

2024 Cybersecurity Outlook Survey

Value Proposition

Raise awareness of Municipal Cybersecurity

Enable discussions with City Council & Leadership

Support for Business Cases

Be the voice of Municipal Cyber functions

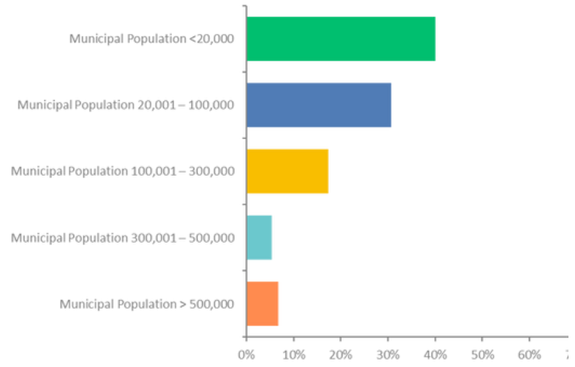
Education and advocacy (e.g., Council, Mayors, Municipal Executives, etc.)

SECTION 1: GENERAL

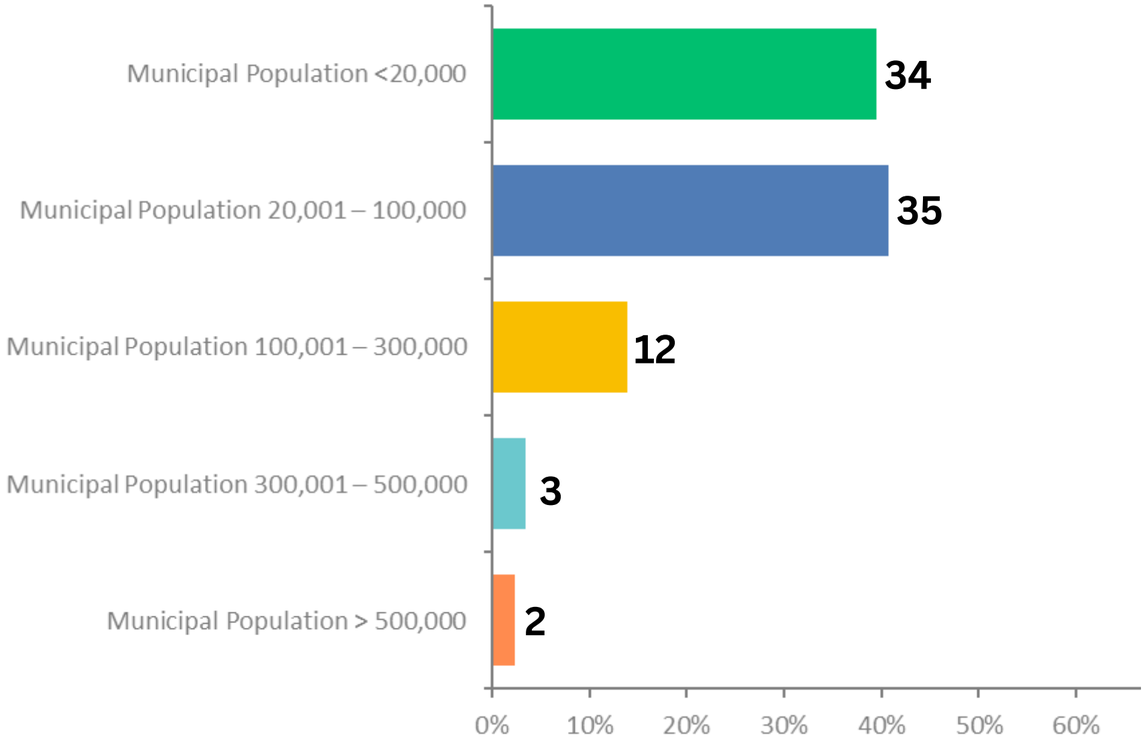
General

Q1 **Population sizes** of participant municipalities

2023



2024

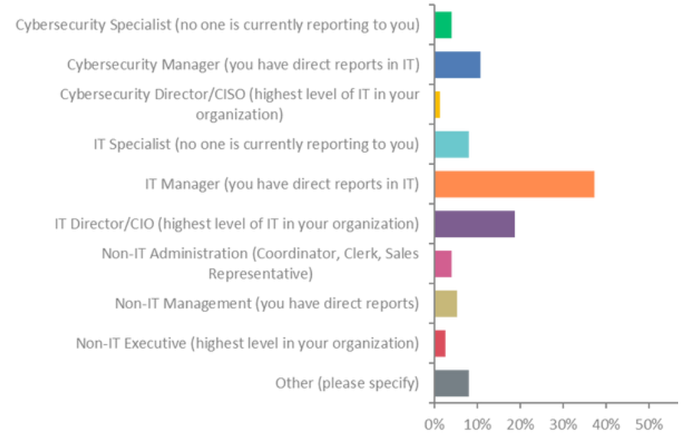


- **80% <100K** population
- **20% >100K** population
- Population **20-100K** shows **greatest increase** of **10%** (23 to 35)

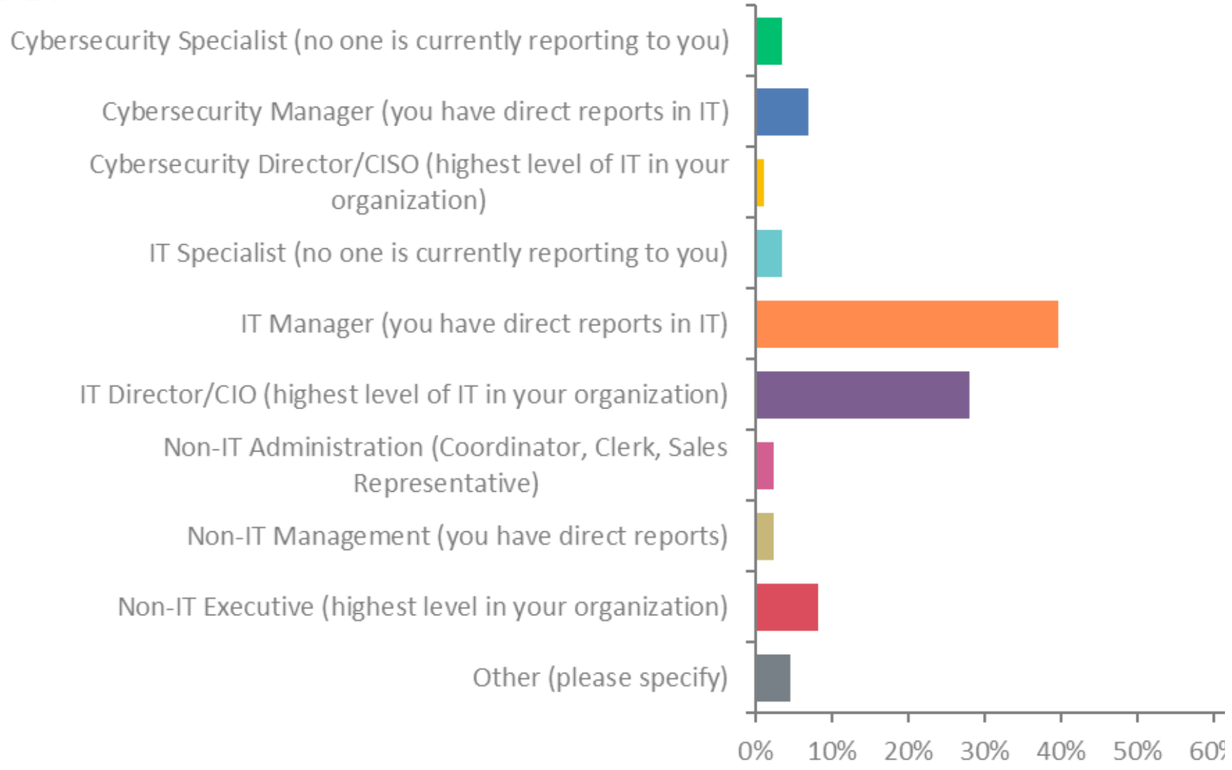
General

Q2 What **position** do you currently hold at your organization?

2023



2024

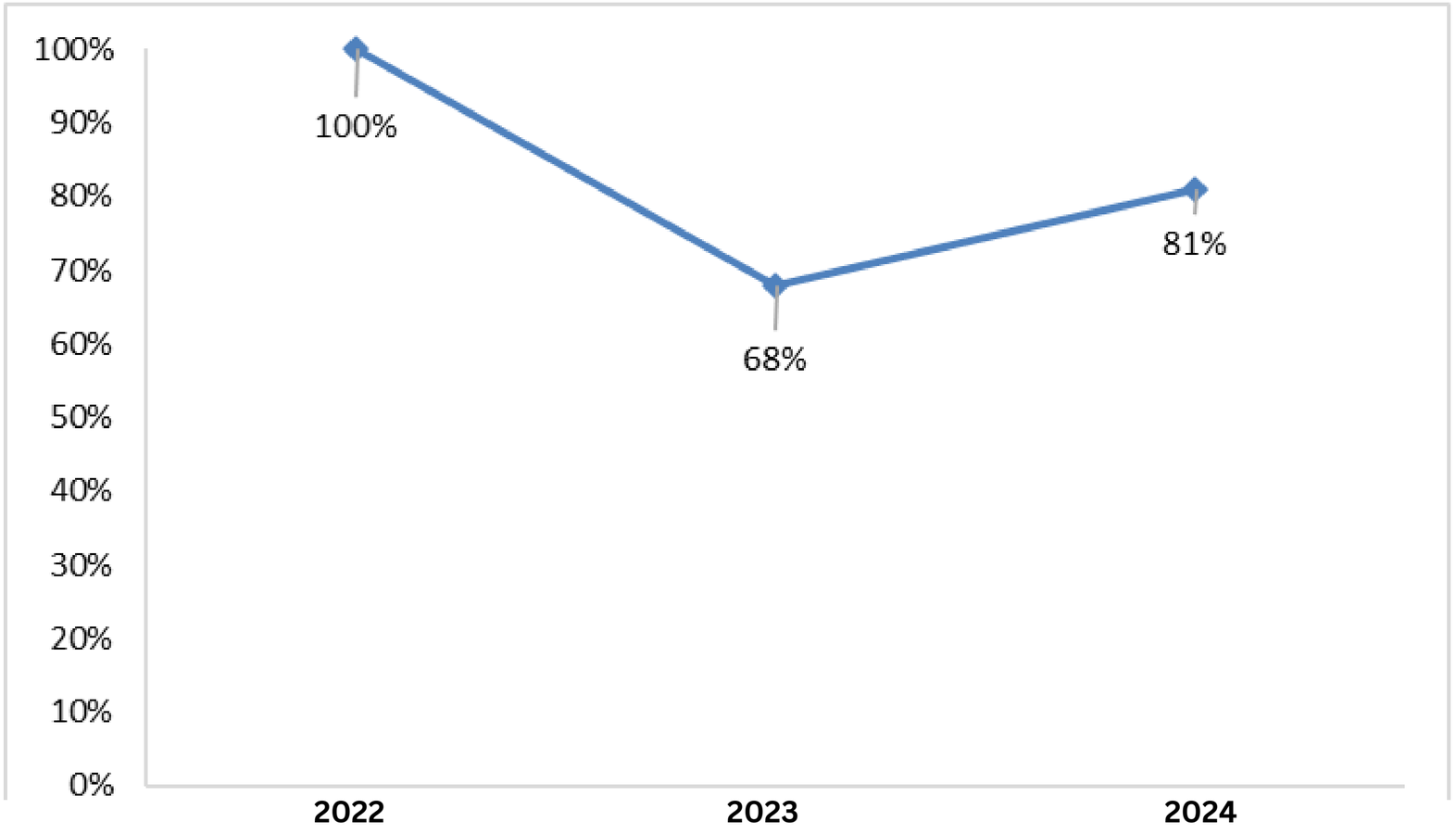


- **83% participants**
  - From **IT/Cyber** functions
- Of the 80%, **67%** are **IT Directors/CIOs/IT Managers**
- **Remaining 17%** are from **non-IT** backgrounds responsible for IT management

SECTION 2: EXECUTIVE BUY-IN

Executive Buy-In

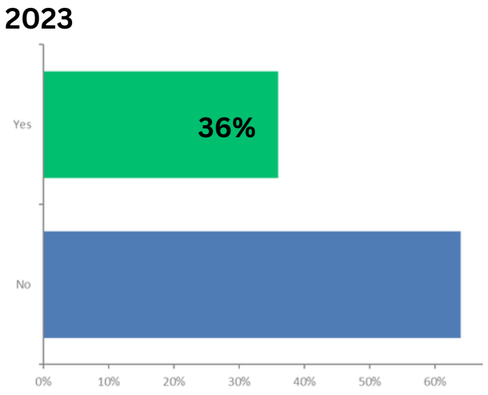
Q5 Does your Municipality **consider** cybersecurity a **top five priority**?

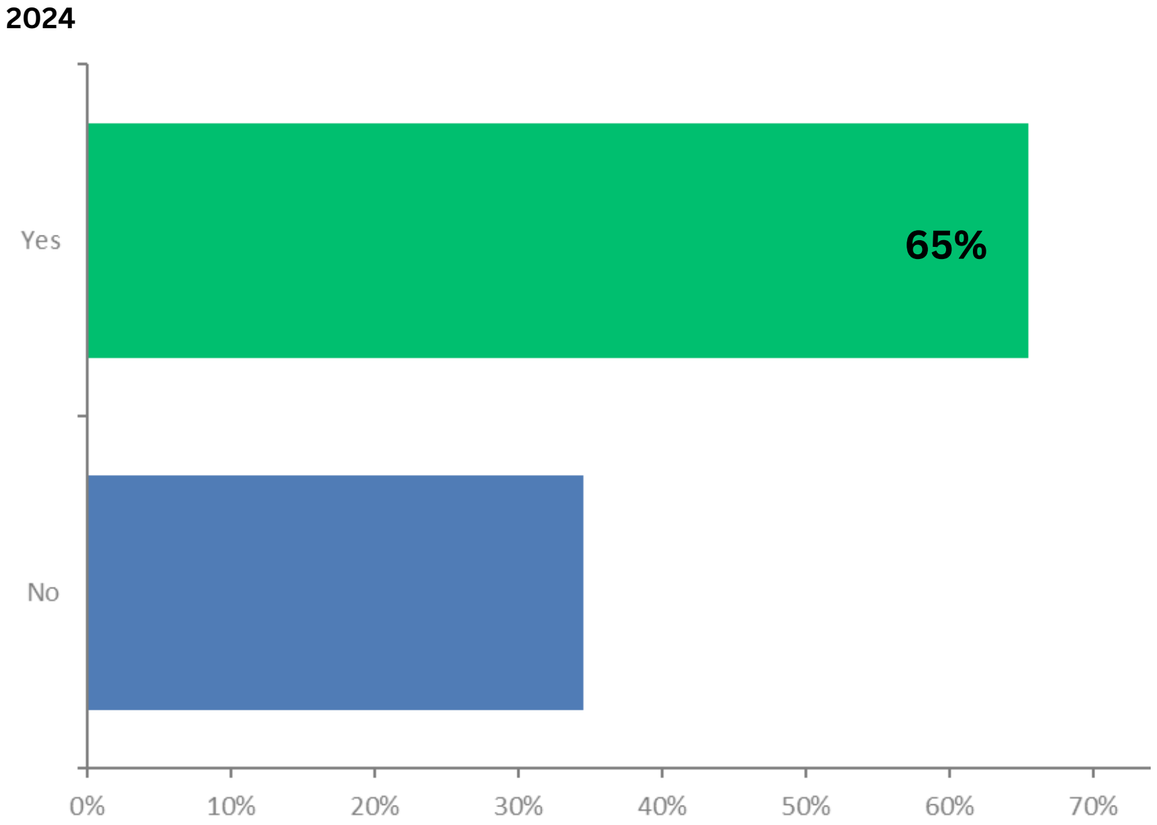


- **81%** municipalities consider **cybersecurity a top 5 priority**
- **2022-2023: Decline** due to **reallocation of finances:** post-Covid19
  - For housing
  - Homelessness
  - Continuity of operations
  - Deferred planned projects
  - Inflation
  - Lower budget increases
  - Reallocation of funding (CAPEX and OPEX), etc.
- **2023-2024: Increase** in **breaches** (e.g., Ransomware)
  - Costs of attack outweigh investment

Executive Buy-In

Q6 Do you **believe** that your **Senior Municipal Executives** are providing the cybersecurity function/division with the **right level of resources/support** for your security program (e.g., funding, people, visible support, etc.)?

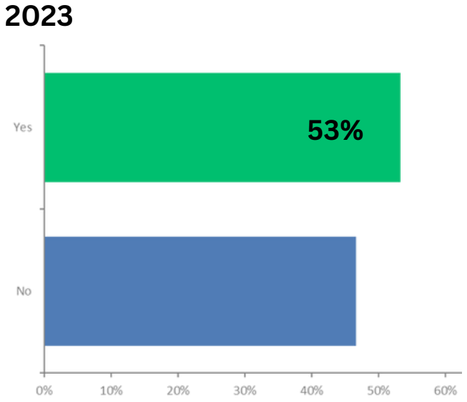


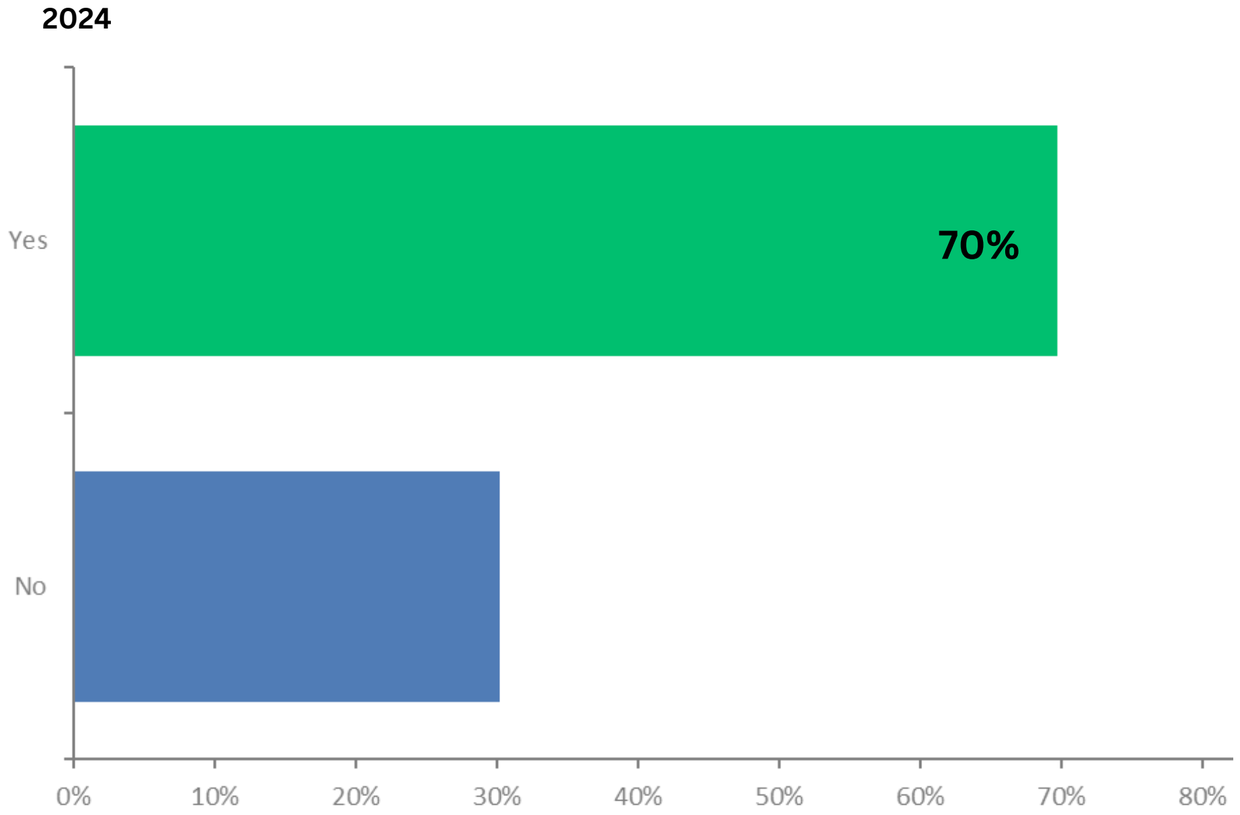


- **65%** of respondents **believe** they have **more support** from Executives in 2024 (**29% increase**)
- **Heightened cybersecurity awareness**:
  - MISA ON
  - Media (reported breaches)
  - Community of Organizations

Executive Buy-In

Q7 Do you **believe** you are provided the **right level of visibility** to the Mayor and Council regarding cybersecurity matters at your Municipality?

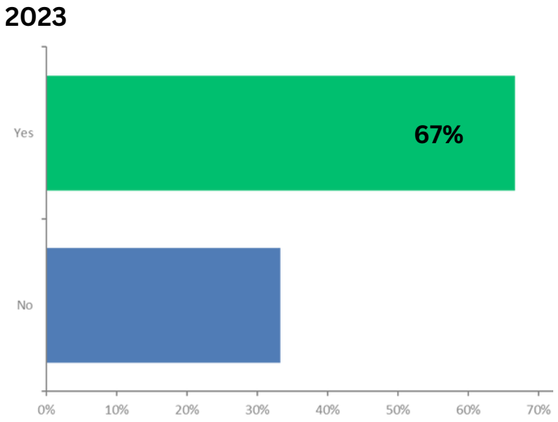


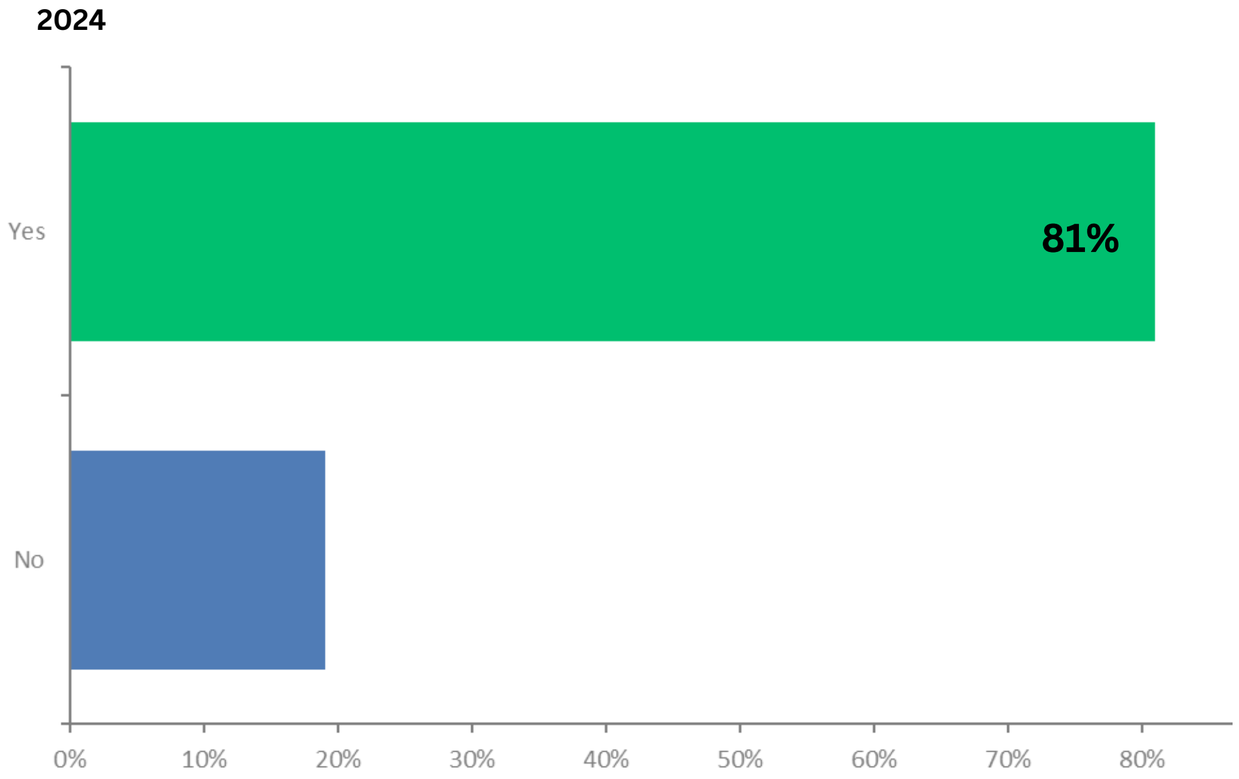


- **70% believe** they have the right level of visibility
- **16% increase** from 2023
- **Increase** of several **high-profile municipal breaches** reported in the media
- Via chain of command
- AI unknowns (sparks conversation)

Executive Buy-In

Q8 Does your Municipality **track and report** cyber **breaches** to Senior Executives, Council or the Mayor's Office?

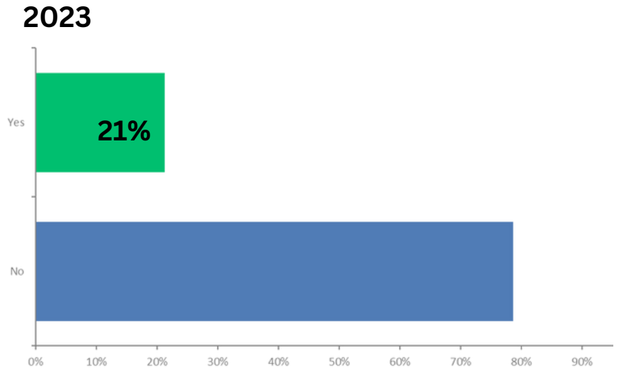


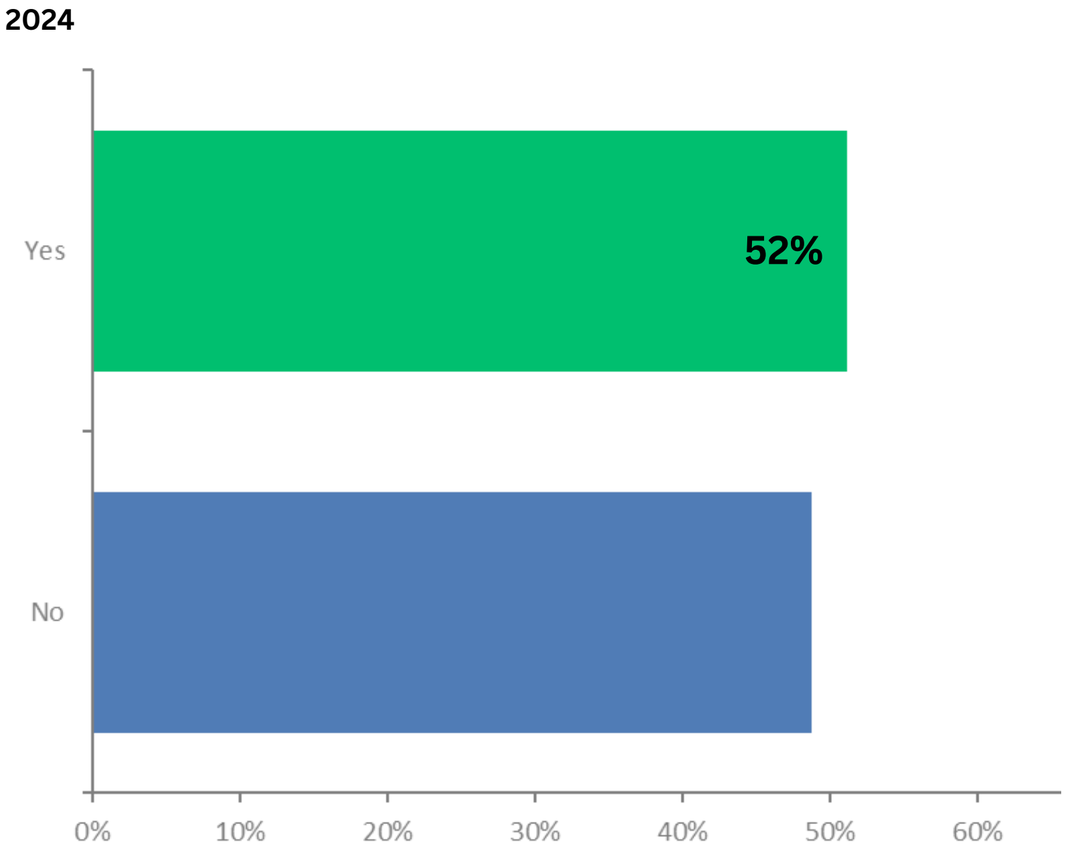


- **81%** of municipalities **report cyber breaches** internally
- This represents an **increase of 15%**
- **Higher priority:**
  - Increased **media coverage**
  - **Bill 194** awareness
  - **Agenda item** for Council
  - **Awareness outreach** from **Province/CCCS**

Executive Buy-In

Q9 Does your Municipality **report** any cybersecurity **metrics** to your Senior Executive/Council/Mayor?





- **52%** municipalities **report cyber metrics** internally
- **A significant increase** of **31%** from 2023
- **Cyber posture maturity**, High-profile **breaches**, **Value for investment**

Key metrics reported:

- **Vulnerabilities**
- **Phishing**
- **Critical risks remediation (monthly)**
- **Maturity Benchmark**

SECTION 3: CYBER FUNCTION

Cyber Function

Marginal Changes

*Q10 Does your Municipality have a **dedicated role** focused on cybersecurity?

- **72% do not** have dedicated roles for cybersecurity

*Q11 Does your Municipality have a **centralized cybersecurity** function ?

- **65%** of the surveyed municipalities **do not** have a cybersecurity function/division

*Q12 Does your Municipality have cybersecurity function that reports into a non-technical role today)?

- **15%** municipalities have a centralized cyber function that reports into a into a **non-technical role** today

*Q13 Does your Municipality have cybersecurity function that **reports into IT function today**?

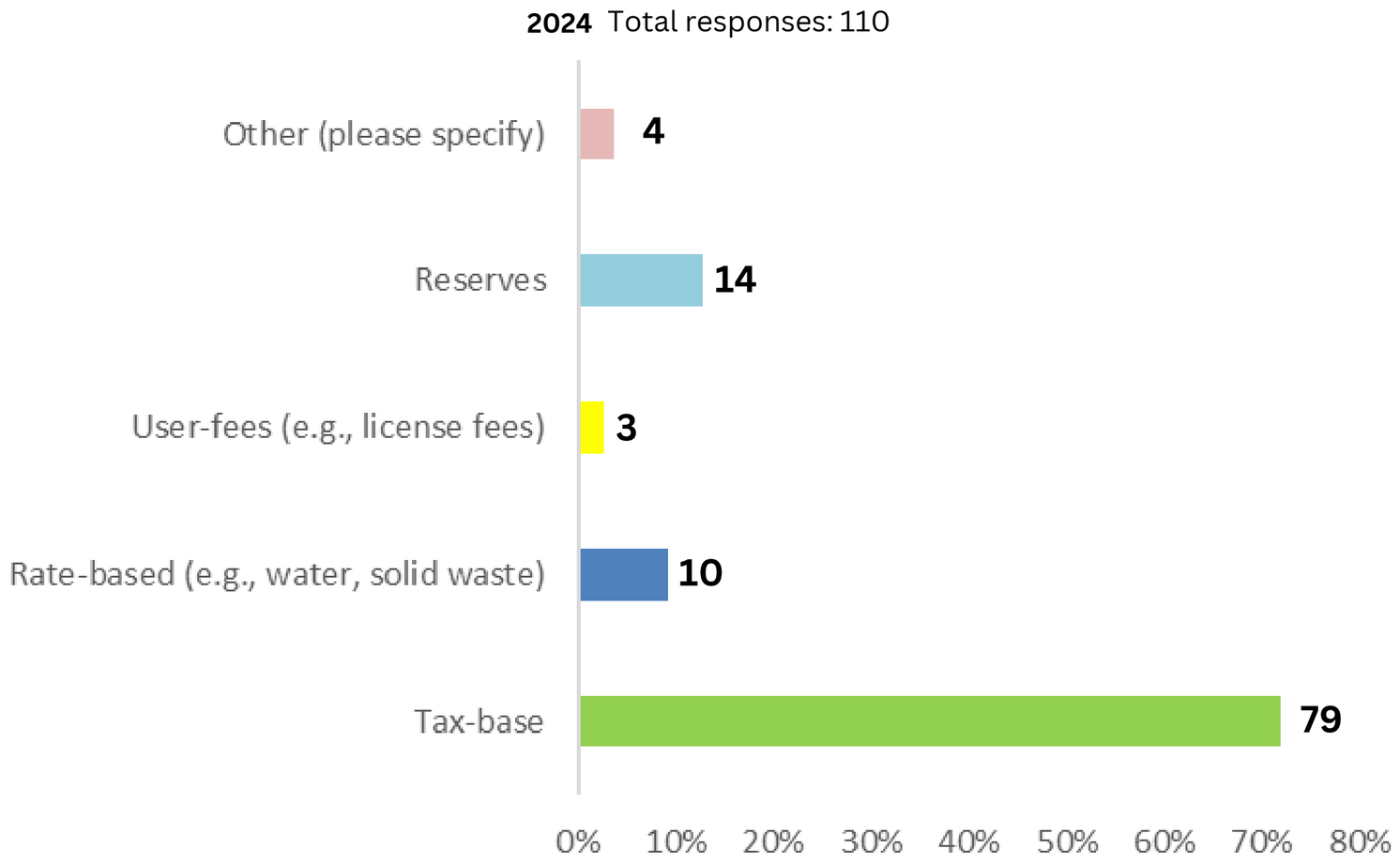
- **49%** municipalities say **YES**

*Questions that show results with less than 10% variation between the 2023 and the 2024 surveys have been grouped together

Cyber Function

NEW

Q14 How is cybersecurity **funded** by your Municipality? (select all that apply)



- **72%** of municipalities **fund cybersecurity** via **Tax-based funding**
- **14%** leverage **Reserves** for funding
  - **Why?**
    - **Change in scope – budget increase**
    - **Not add to tax-base burden**
    - **Grants sitting in reserve**

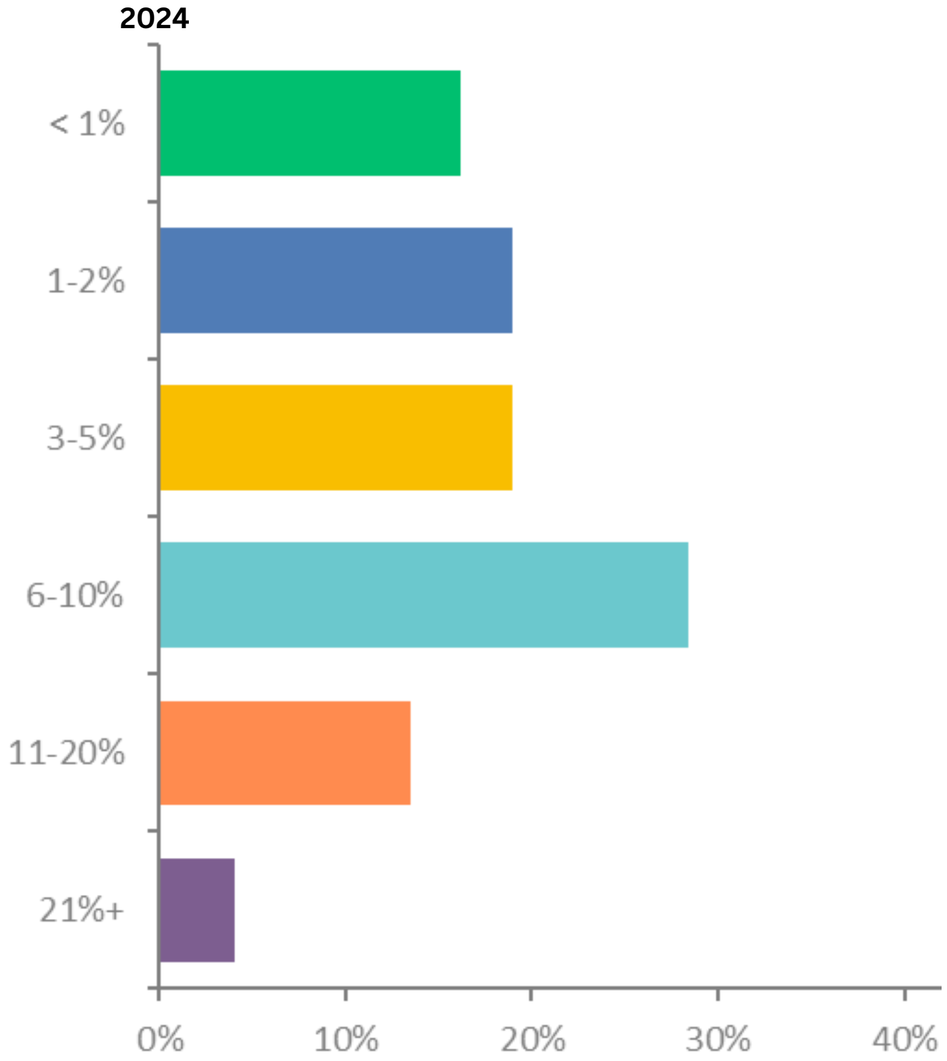
Multiple selections allowed

Cyber Function

Q15 For your Municipality, is your **cybersecurity budget** part of the **IT budget**?

- **88%** of municipalities **have** their cybersecurity budget **as part of the IT budget**

Q16 What percentage is **allocated to cybersecurity?**

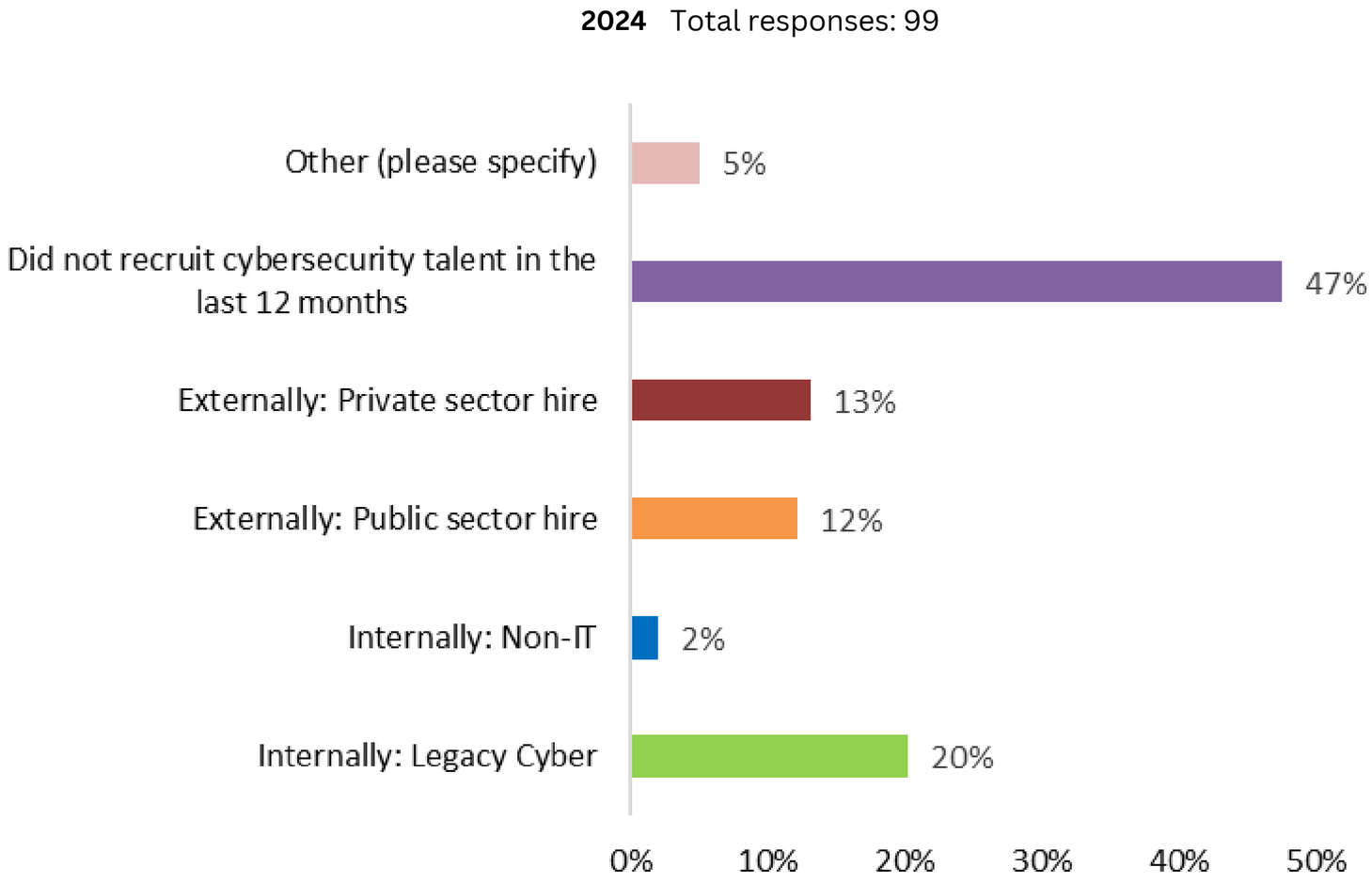


- **54%** of municipalities have allotted **<5% of their IT budget to cybersecurity**
- **Increase in allocation** of cybersecurity budgets of **>5% from 2023**
- **Shifting spend** (capital funding)
- **Hiring IT resources with cyber skills** or developing skills
- **Complimentary resources** from **Province/CCCS**

SECTION 4: TALENT

Talent

Q17 Was your **cybersecurity talent recruited** internally or externally? (select all that apply)

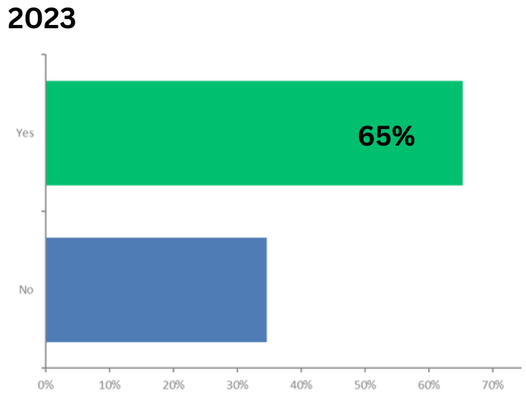


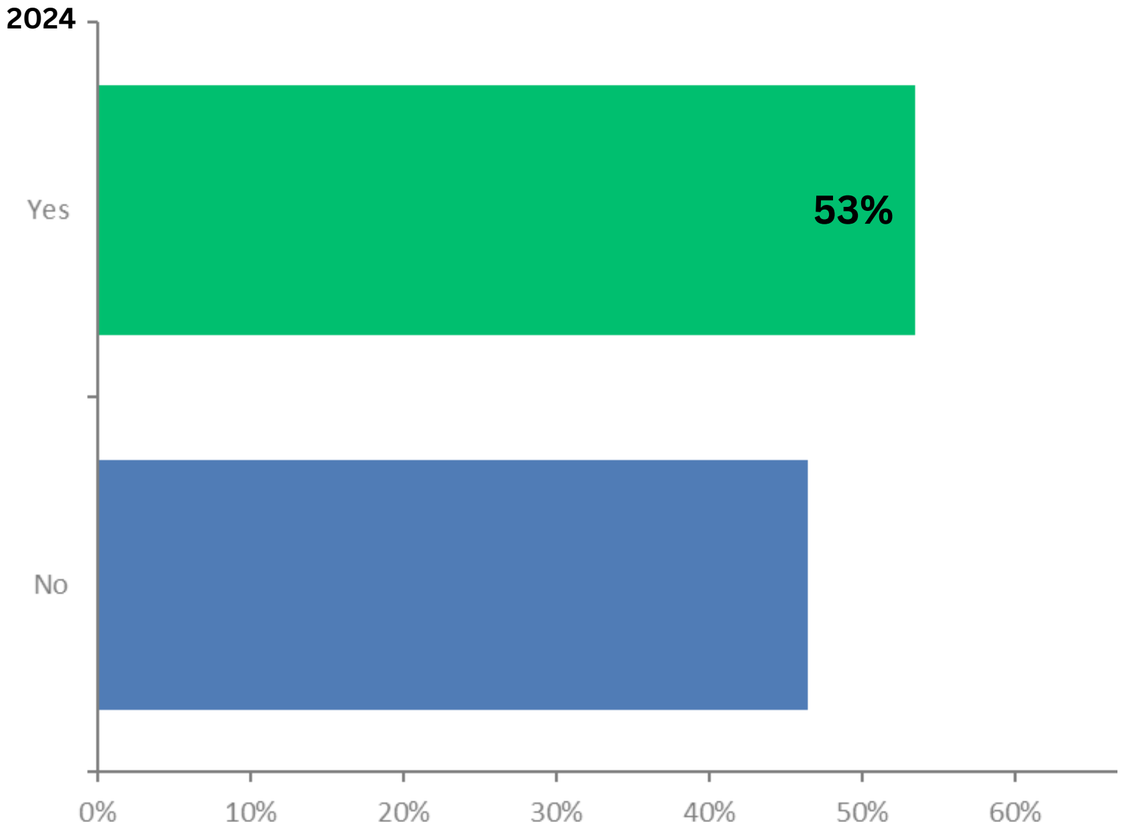
- **47%: No recruitment** in 2024
- Of those that recruited:
  - **22% Internal**
  - **25% External**
- **Smaller municipalities** may hire **external due to budget**
- **Many** municipalities **have both internal and external MSSPs**

Multiple selections allowed

Talent

Q18 In general, do you **believe** your Municipality would **benefit** (e.g., cost savings, local talent development, etc.) from **reducing the number of third-party contractors** (e.g., independent, larger consulting firms and vendors) in favour of full-time permanent staff?

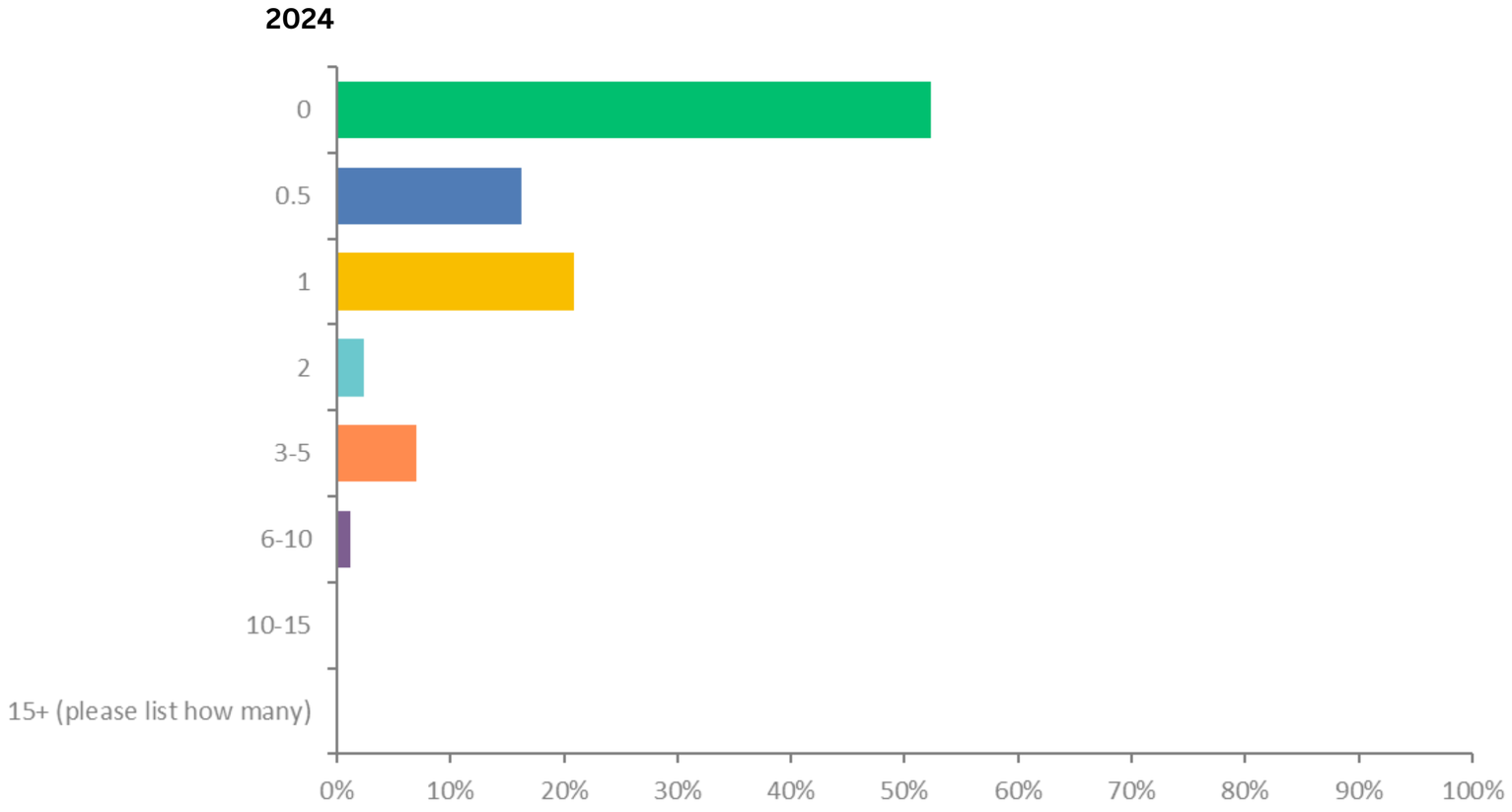




- **53%** of municipalities would benefit from reducing third-party contractors
- This represents a **decrease in 12%** from 2023
- Municipalities are **favoring third-parties vs. staff**

Talent

Q19 How many **dedicated cybersecurity management and staff** does your Municipality have today?



- **52%** of municipalities **DO NOT** have **dedicated** cyber talent
- **37%** of municipalities have **less than 1 dedicated cybersecurity staff**

SECTION 5: CHALLENGES

Challenges

Q20 What are the **top three general security challenges** your Municipality is facing?

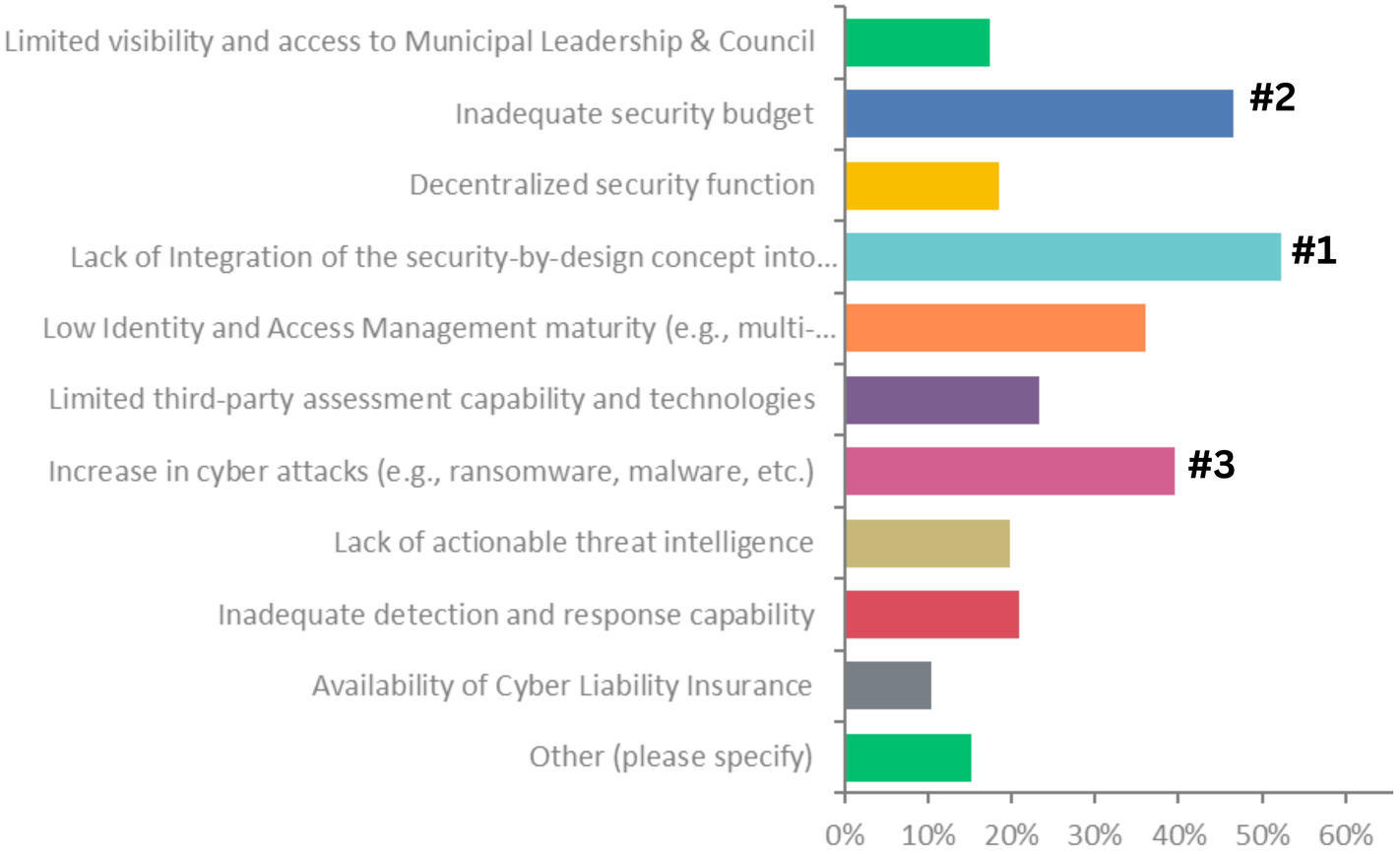
2023

1. Inadequate **security budget & security-by-design**

2. Increase in **cyber attacks**

3. Low **IAM maturity**

2024



1. Lack of **security-by-design**

2. Inadequate **security budget**

3. Increase in **cyber attacks**

Challenges

Q21 What are the **top three cybersecurity operational challenges** for your Municipality?

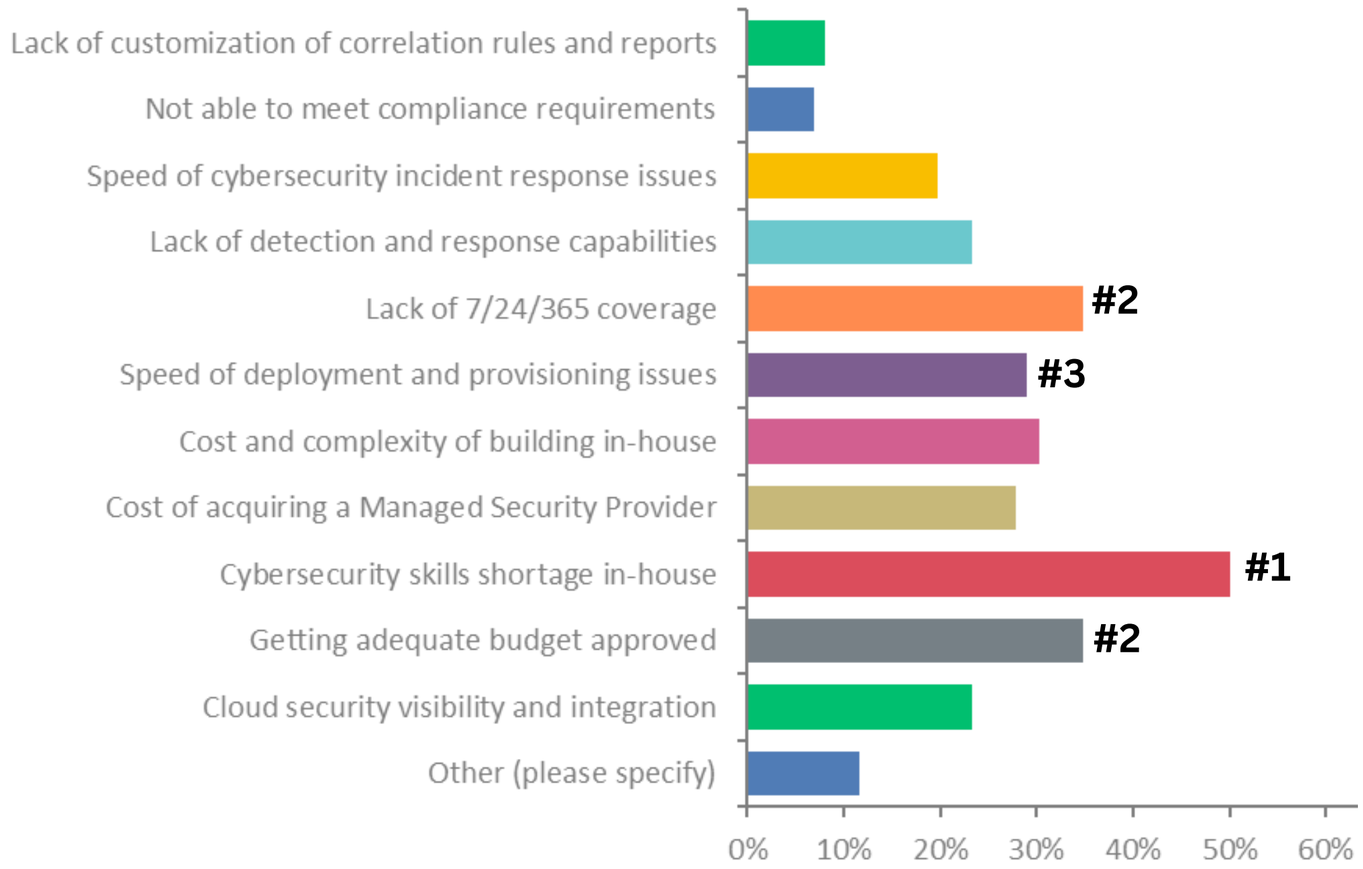
2023

1. Cybersecurity **skills shortage**

2. Lack of **7/24/365 coverage**

3. Lack of **detection and response capabilities**

2024



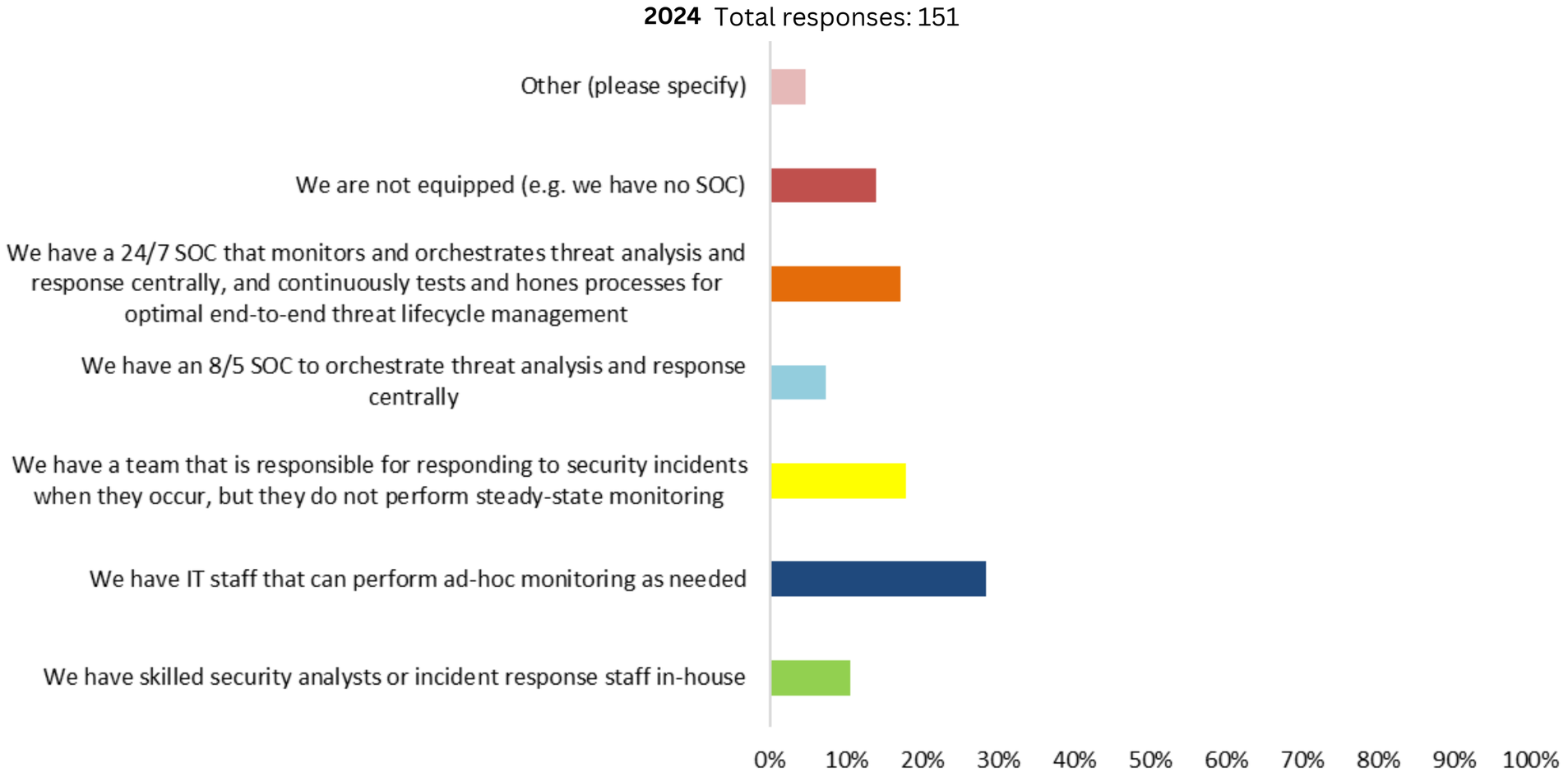
1. Cybersecurity **skills shortage** in-house

2. Lack of **7/24/365 coverage**, Getting **adequate budget**

3. Speed of **deployment and provisioning issues**

Challenges

Q22 How **equipped** are your Municipal staff and processes to **deal with incoming threats**? (select all that apply)



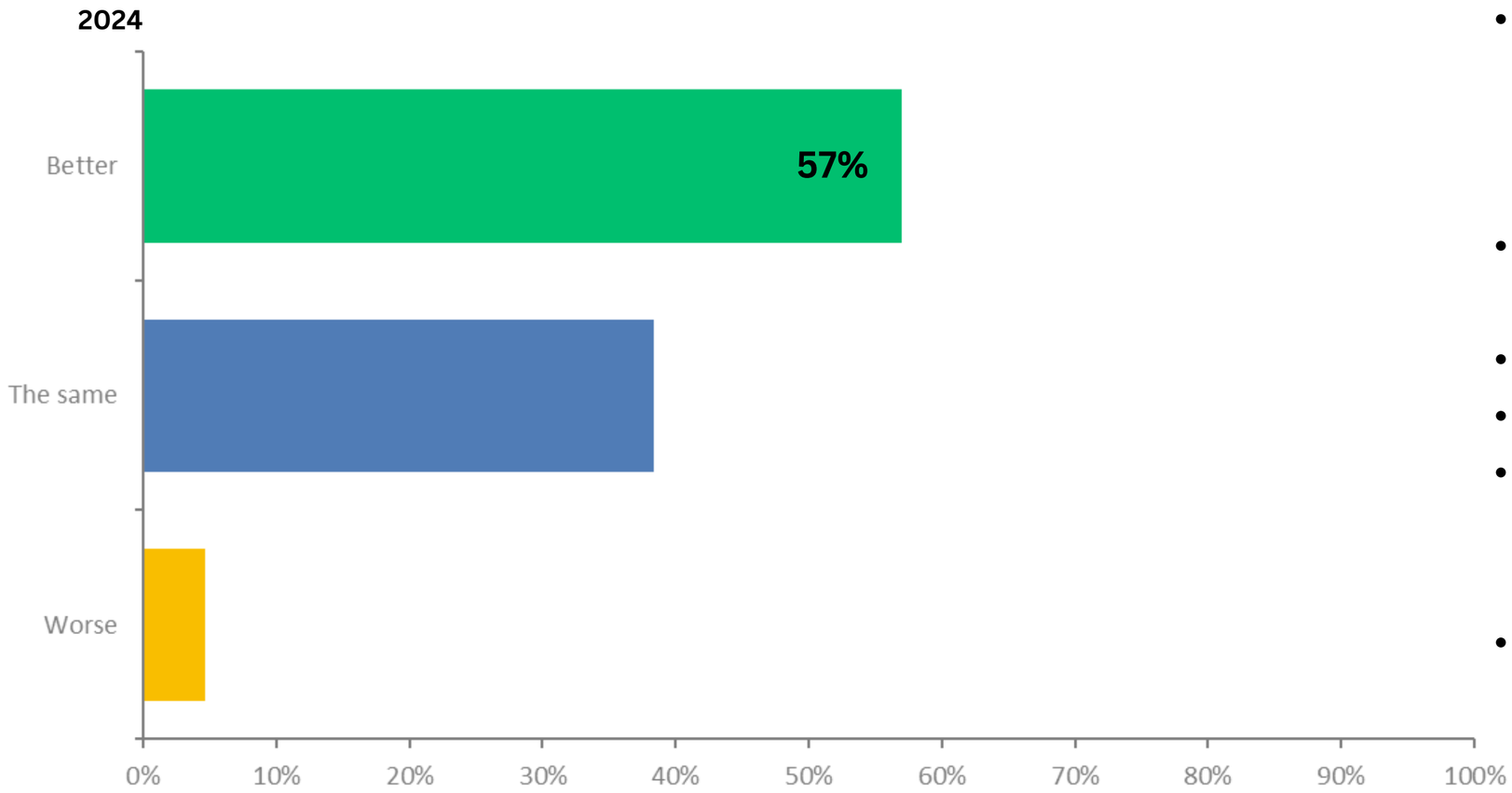
- **81%** of municipalities perform **monitoring**
  - **46% ad-hoc**
  - **35% formal**
- **14%** of municipalities have **no monitoring capabilities**

Multiple selections allowed

Challenges

NEW

Q23 In the last year, how do you **feel** about your Municipality's **ability to respond to a cyberattack**? (compared to 2023)



- **57%** of municipalities feel **better equipped** to respond to cyberattacks

- **Awareness, training, funding, resources**
- **Reporting metrics**
- **Prepared IR plans and testing**
- **Municipalities sharing their lessons learned at MISA conferences**
- **Peer groups: CISO SIG group, CCCS calls**

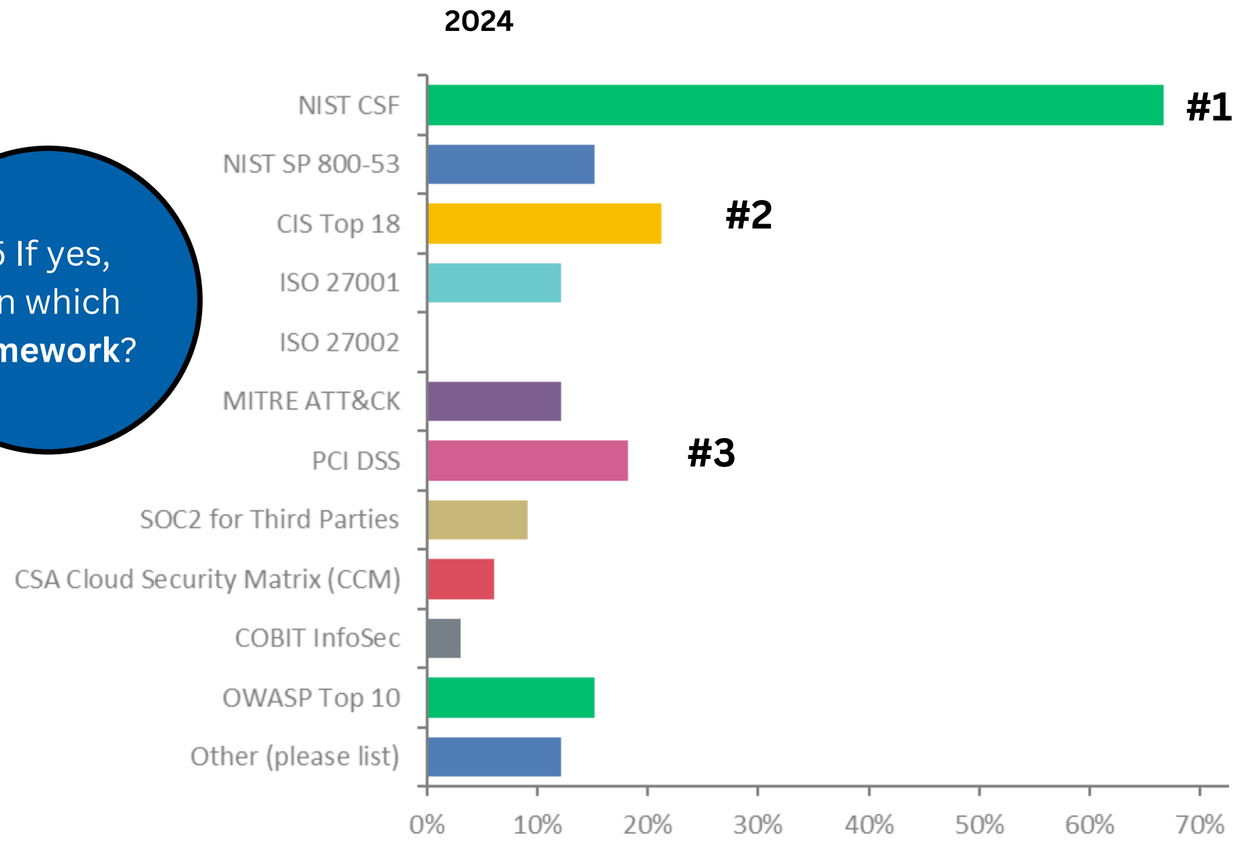
SECTION 6: CYBER FRAMEWORK

Cyber Framework

Q24 Does your Municipality currently **adhere to**/implemented any **cybersecurity framework or leading practice** (e.g., NIST CSF, ISO 27001, etc.)?

- **38%** of municipalities adhere to cybersecurity framework/leading practice
- **9% increase** from 2023

Q25 If yes, then which **framework**?



1. **67% NIST CSF**
2. **21% CIS Top 18**
3. **18% PCI DSS**

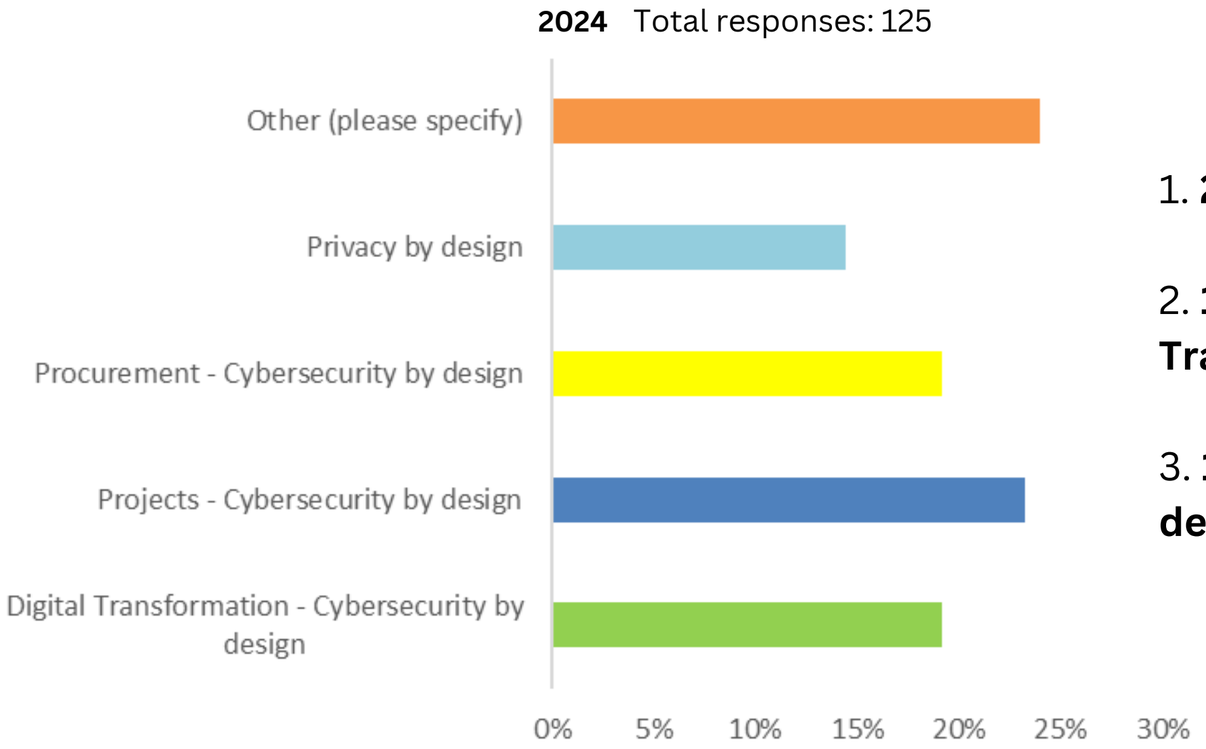
- **Greatest decrease** from 2023 in adhering to **ISO 27001 (24%) and ISO 27002 (22%)**
- Moving to **more practical and pragmatic frameworks**
- **NIST CSF: dynamic, more globally adopted, has frequent updates**

Cyber Function

Q26 In general, do you **believe** Municipalities should **integrate cybersecurity and privacy by design principles** into all transformations, initiatives/projects and procurement? (select all that apply)

- **90%** of municipalities **believe** they **should** integrate cybersecurity and privacy by design principles

*Q27 If yes, has your Municipality **embedded "by design"** principals? (Select all that apply)

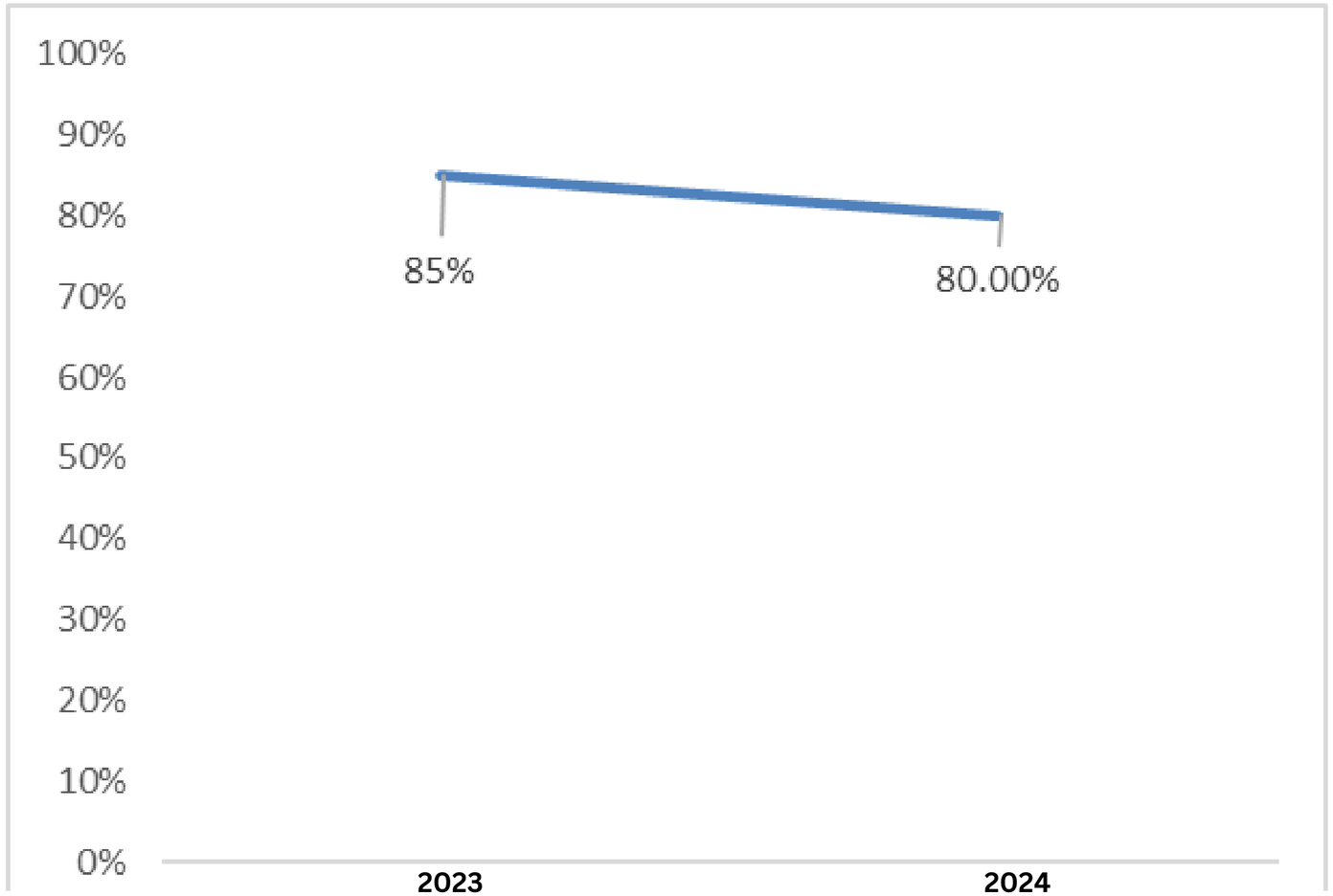


1. **23% Projects**
2. **19% Digital Transformation**
3. **14% Privacy by design**

*Multiple selections allowed

Cyber Framework

Q28 Do you **believe** that there should be **regulation** introduced to govern Municipal cybersecurity?



- **80%** municipalities **agree** a regulation governing Municipal cybersecurity **should be introduced**
- **5% decrease** from 2023:
  - **Realization of impacts**: **Bill 194**

SECTION 7: CITIZENS

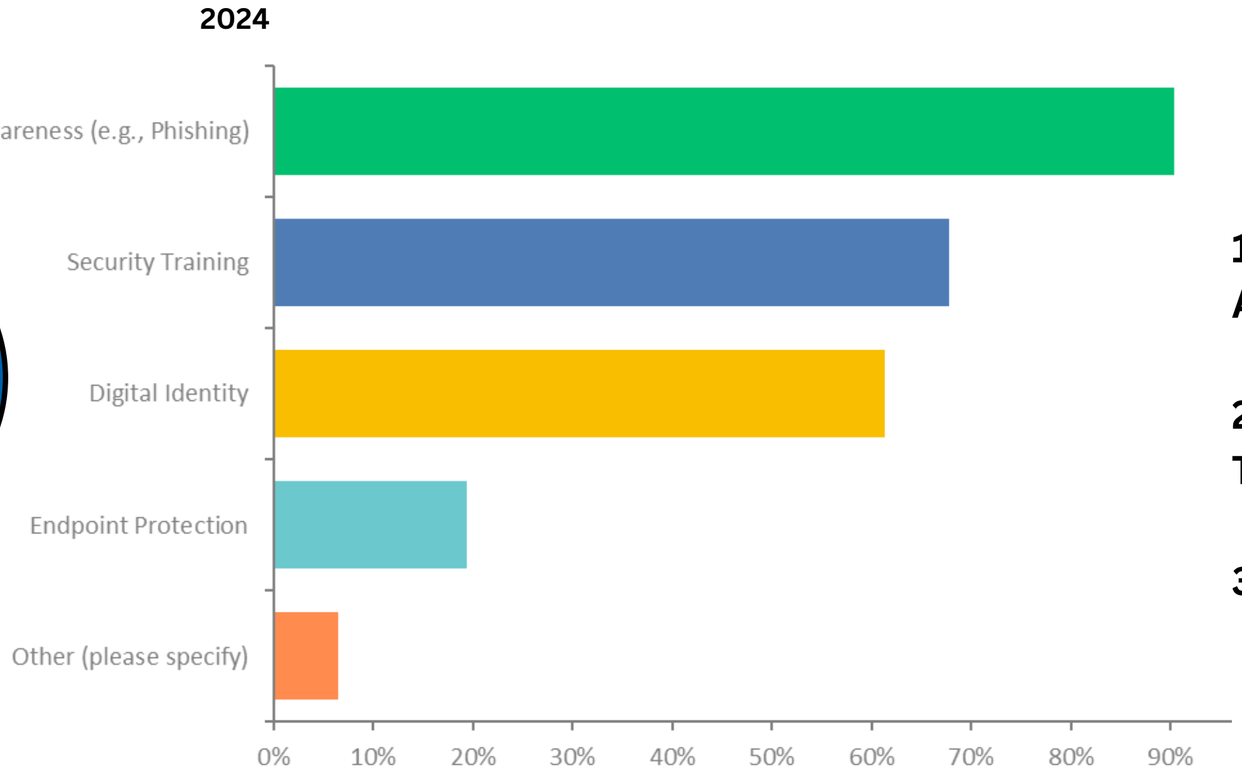
Citizens

Q29 In general, do you **believe** that Municipalities should develop/**provide** new innovative **security services directly to citizens** (e.g., awareness, digital identities, cyber guidelines, endpoint protection, etc.)?

- **36%** of respondents **believe** municipalities **should** provide security services directly to citizens

- **21% increase** from **2023 (15%)**

Q30 If yes, what type of security services



1. 90% Security Awareness

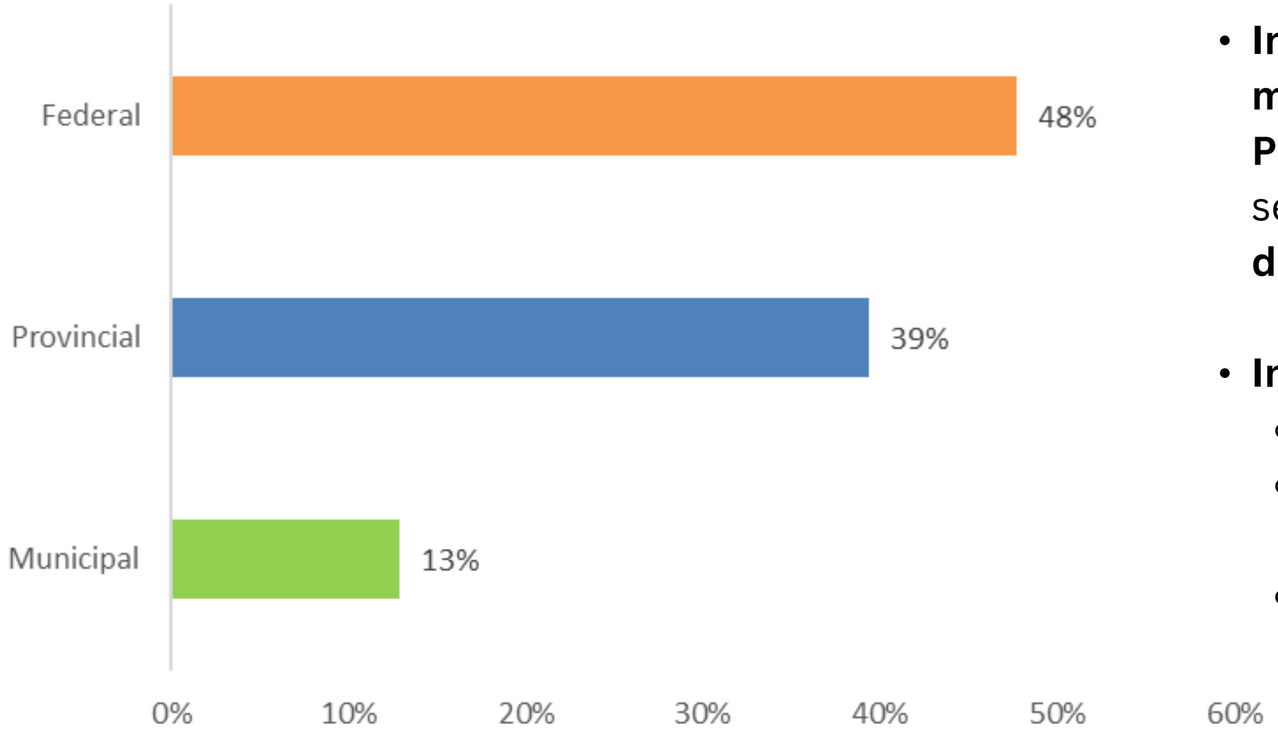
2. 68% Security Training

3. 61% Digital Identity

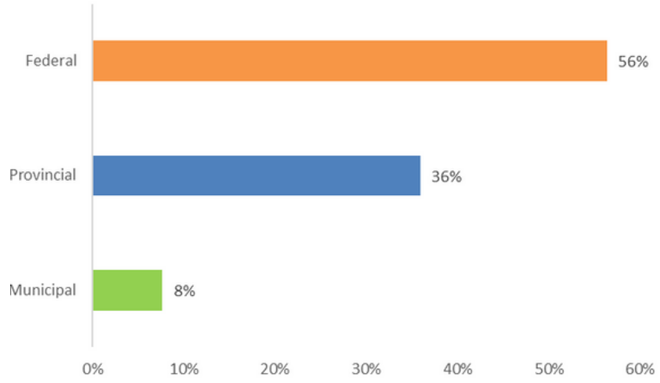
Citizens

Q31 In general, do you **believe** that providing security services directly to citizens is a **responsibility** of **Municipalities, the Province of Ontario, and/or the Federal Government**? (select all that apply)

2024 Total responses: 155



2023 Total responses: 117



- **Increased belief** that **municipalities and the Province** should be serving their citizens **directly (52%)**
- **Increased awareness:**
  - **Governments**
  - **Mayors/Councillors/ Politicians**
  - **Bill 194**

Multiple selections allowed

SECTION 8: BREACH AND RESPONSE

Breach and Response

Cyber liability insurance

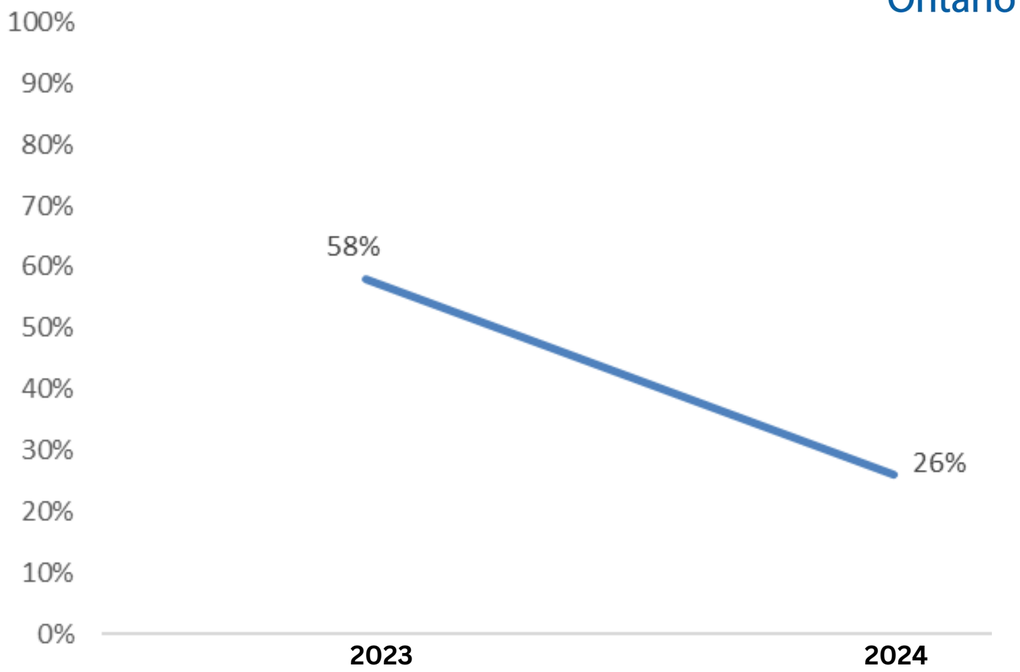
*Q32 In general, do you **believe** it is important for Municipalities to have **cyber liability insurance?**

*Q33 Does your Municipality **currently have** cyber liability insurance?

Q34 If you answered yes, has your Municipality had **challenges acquiring** cyber liability insurance in the past **two years**?

- **Important to have**
  - **86%: YES**
- **Currently have**
  - **77%: YES**

*Marginal change from 2023



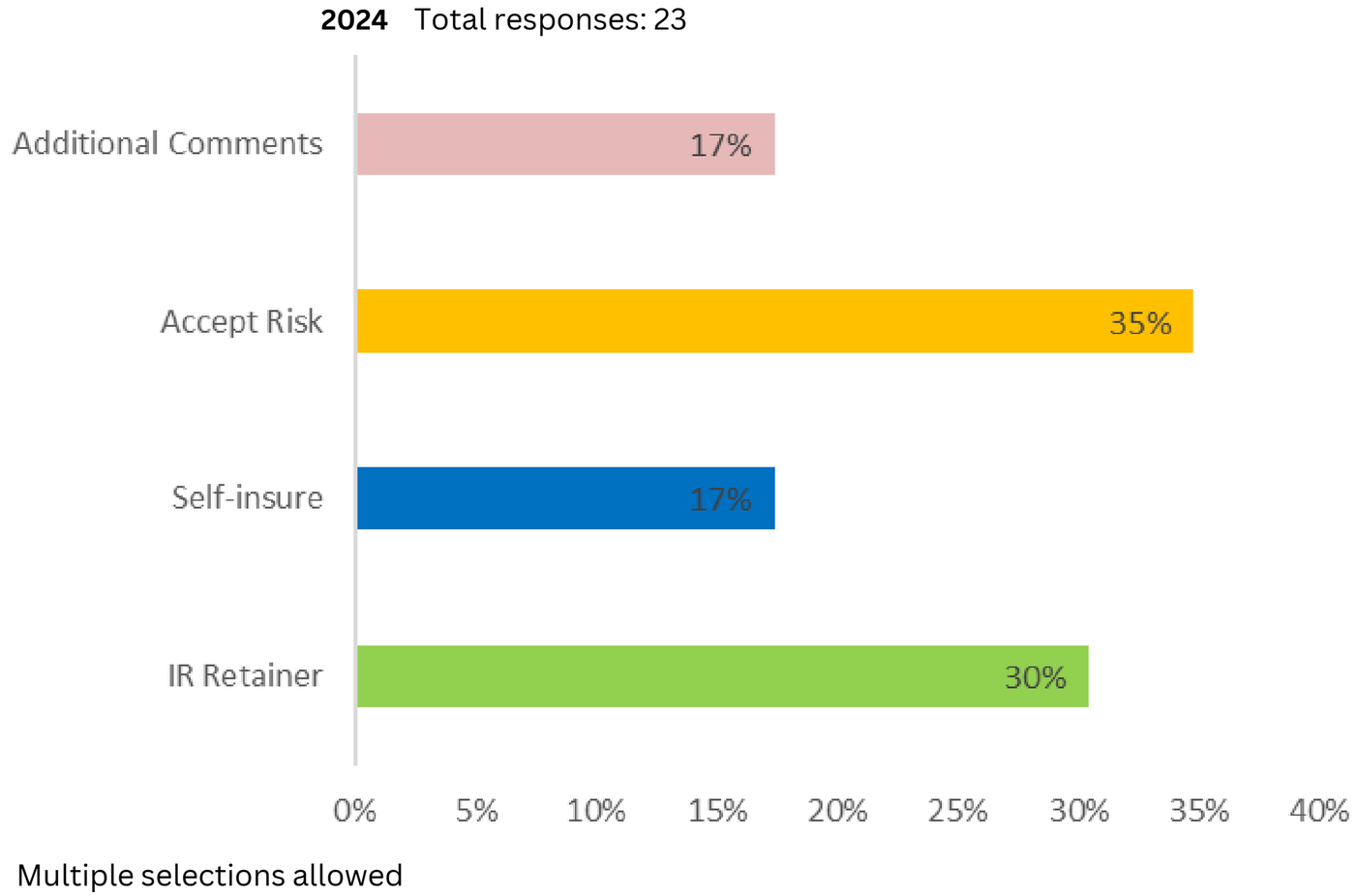
- **32% decrease** in municipalities **facing challenges** acquiring cyber liability insurance
  - **Market has adapted**
  - **Exclusions**
  - **Increase in premiums**
  - **Large deductibles**
  - **Security specialists hired by Insurance providers (same level)**
  - **OT, Industrial Control Systems (SCADA)**

Breach and Response

Cyber liability insurance

NEW

Q35 If no, what **alternative** to **cyber liability insurance** do you have?



Multiple selections allowed

- **52%** municipalities taking an **internal approach:**
  - **35%**: **Accepting risk**
  - **17%**: **Self-insured**

- **Some items being excluded from policy** (e.g., 3rd party breach exclusion and ABCs)
- **Applying funding from cyber insurance to hiring dedicated resource**

- **30%** municipalities taking an **external approach:**
  - **IR Retainer**
  - **3rd party provider** providing insurance (e.g., 1M from DarkTrace)
  - **Shared service between multiple Municipalities (pool one policy)**

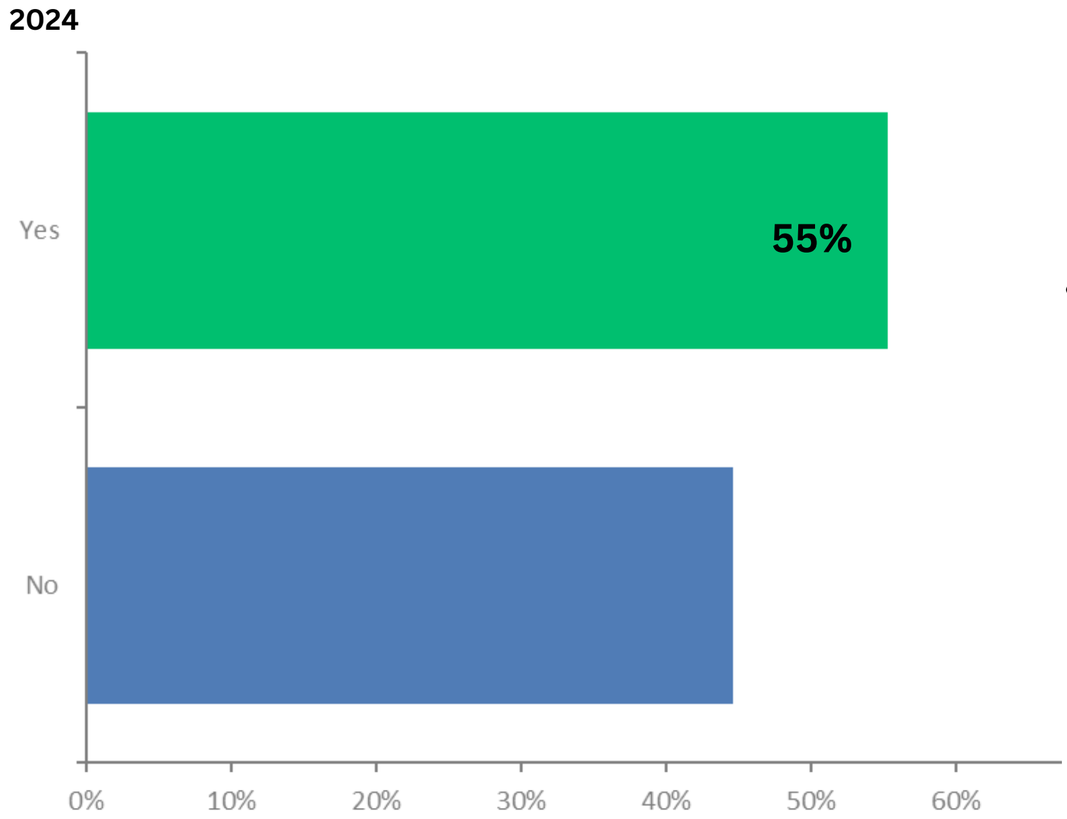
Breach and Response

Cyber Incident Response and Recovery Plan

Q36 Does your Municipality have a **Cyber Incident Response and Recovery Plan** today?

- **55%** of respondents currently **have** a Cyber Incident Plan
- **8% increase** from **2023**

Q37 If yes, does your Municipality **conduct annual tests** to ensure operational effectiveness?

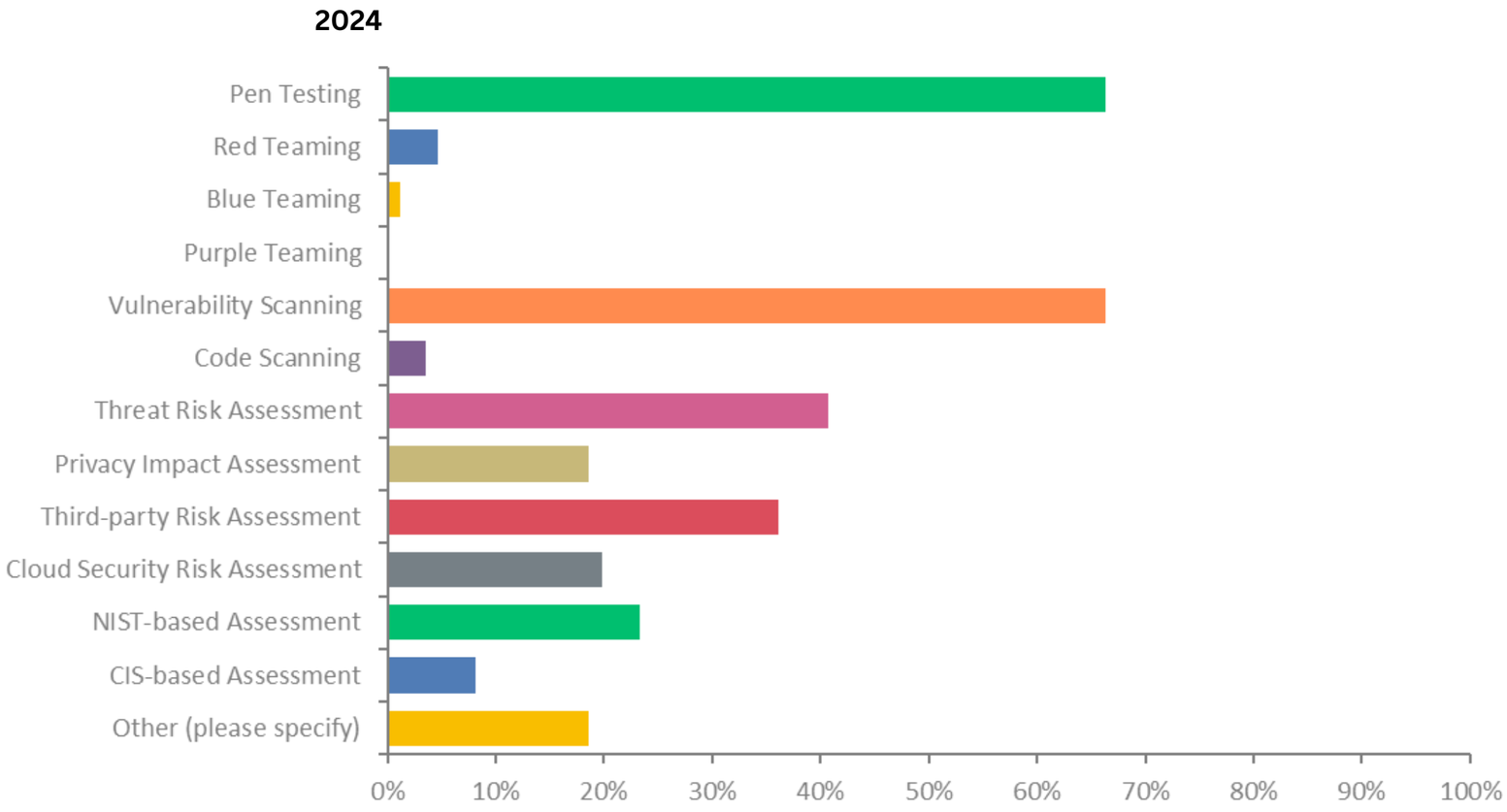


- Of the municipalities with a Cyber Plan, **55% annually** test it

Breach and Response

Cyber Incident Response and Recovery Plan

Q38 Does your Municipality **conduct** any cybersecurity **assessments or tests** to mitigate risk?



- **Top 3** assessments **remain the same** from 2023:
  - **68% Vulnerability Scanning**
  - **66% Pen Testing**
  - **40% Threat Risk Assessment**

- **Third-party risk** has risen over 3 years, prompting municipalities to **increase third-party assessments** by 14% since 2023

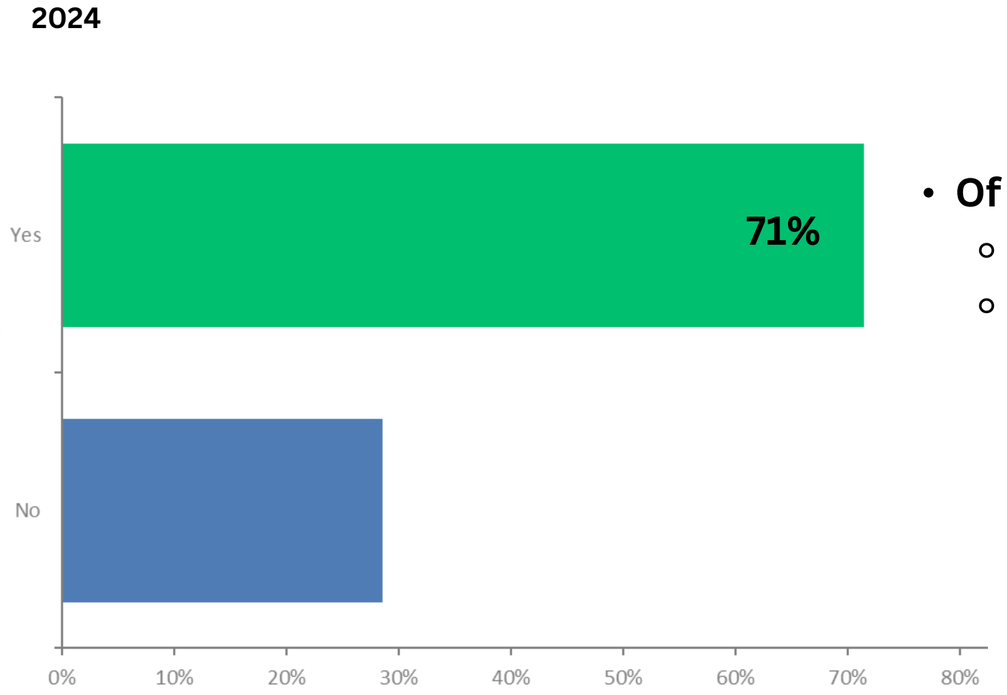
Breach and Response

Material Cyber Breach

Q39 Has your Municipality experienced a **material cyber breach** in the **past two years** (e.g., ransomware) resulting in **significant** financial costs or operational disruption?

- **6% of** municipalities **have** experienced a **material cyber breach** in the past two years
- ***3% decrease** from 2023 **(9%)**
- **Min. 27/444** municipalities **potentially** breached (extrapolation)

Q40 If you answered **yes**, and have experienced a breach, did you **have cyber liability insurance**?



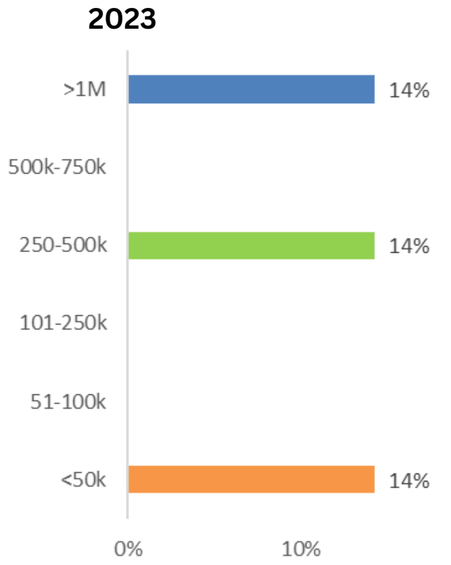
- **Of the 6% breached**
  - **71%** insured
  - **29%** not insured
    - **Self-recovery and resourcing**
    - **~$250K-7M**

***In 2023, we focused on any breach. In 2024, adjusted question to focus on material breach with significant impact**

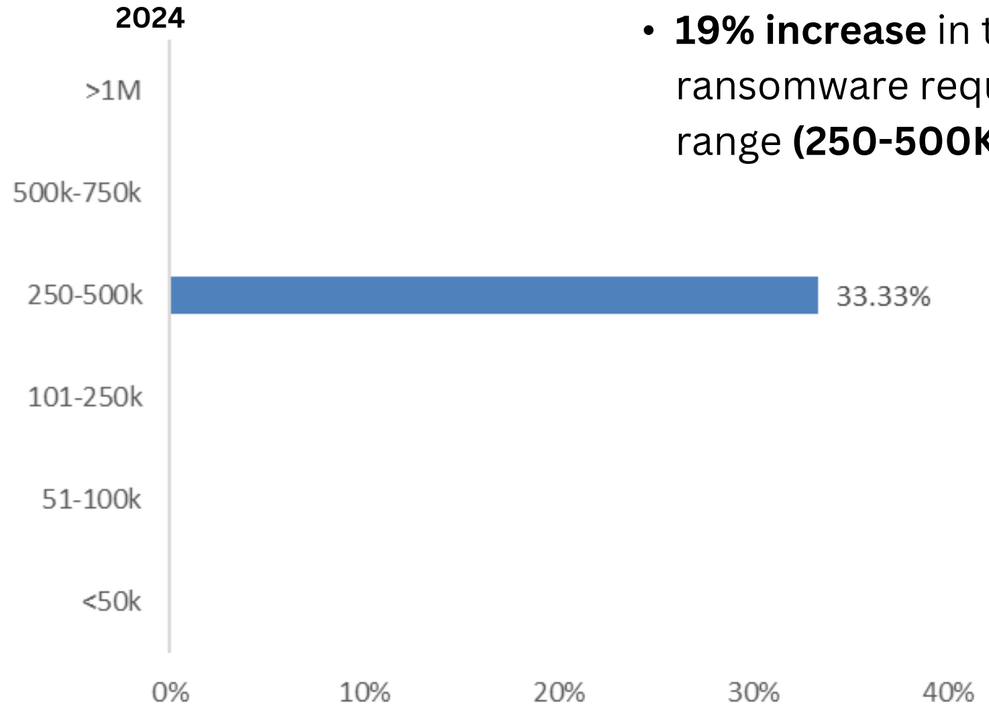
Breach and Response

Material Cyber Breach

Q42 If **yes**, and if you suffered a **ransomware event**, how much was the **initial ransom request** for?



- **14%** of municipalities **each** recorded:
  - **<50K**
  - **250-500K**
  - **>1M**



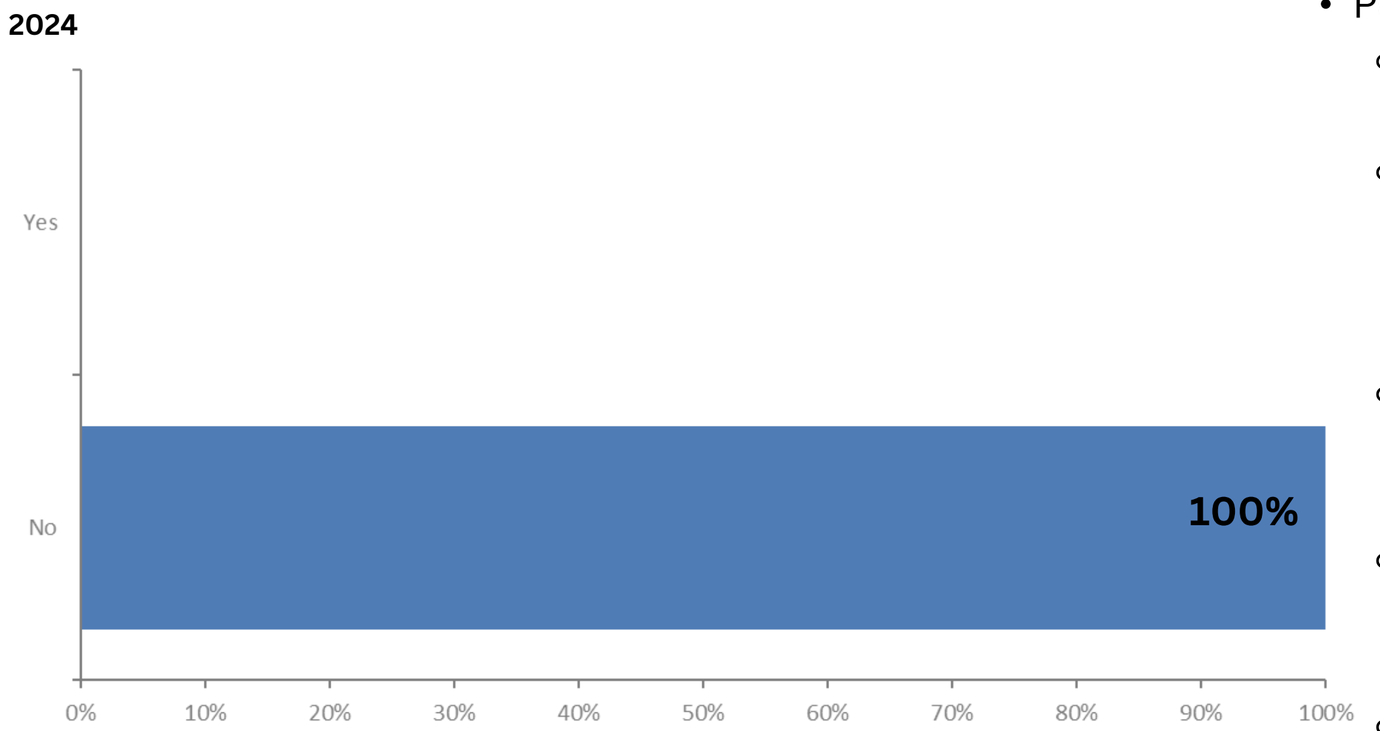
- **33%** of municipalities recorded: **250-500K** initial ransom request
- **19% increase** in this ransomware request range **(250-500K)**

Breach and Response

Material Cyber Breach

NEW

Q43 If **yes**, and if you suffered a **ransomware event**, **did you pa**y the ransom?



- **100%** of municipalities **DID NOT** pay the ransom
- Potential **reasons**:
  - **Cyber insurance**
  - If **self-insured**, **recovery funding in reserves**
  - **Decisions from Mayor/Council**
  - **Third-party IR Retainer**
  - **Reputation**
  - **Recovery viable**

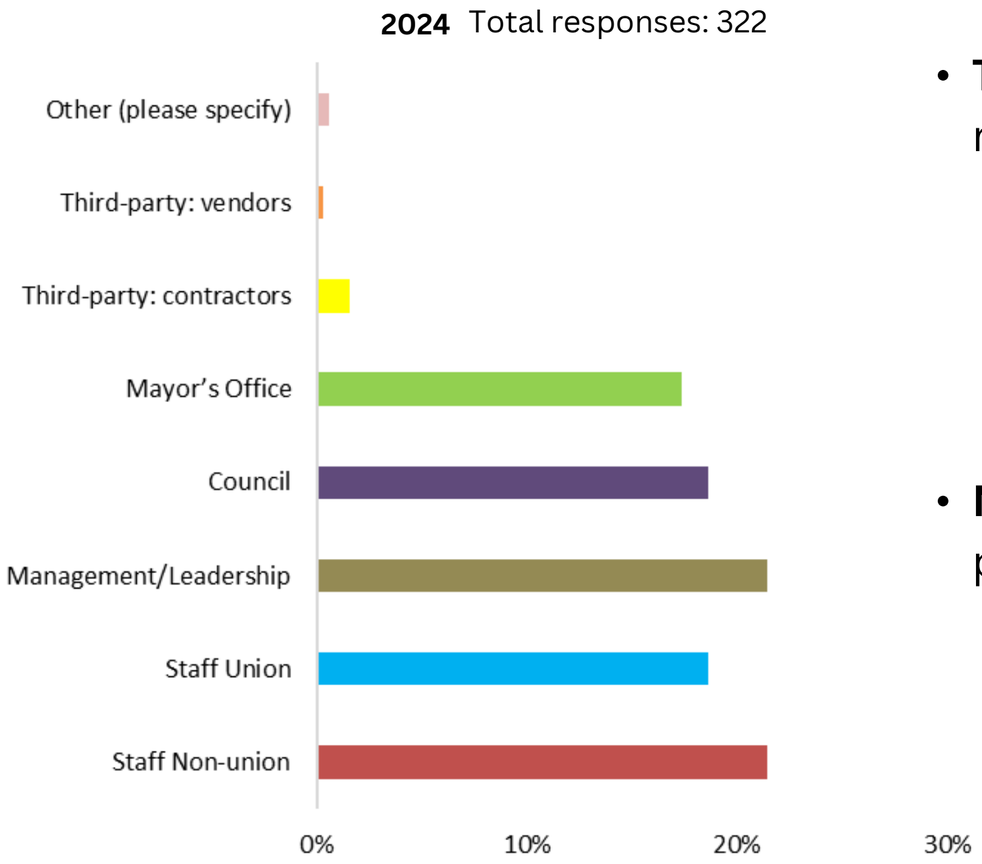
SECTION 9: AWARENESS AND TRAINING

Awareness and Training

Q44 Does your Municipality have a cybersecurity **awareness and training program**? (select all that apply)

- **80%: YES**
- **4% increase** from 2023

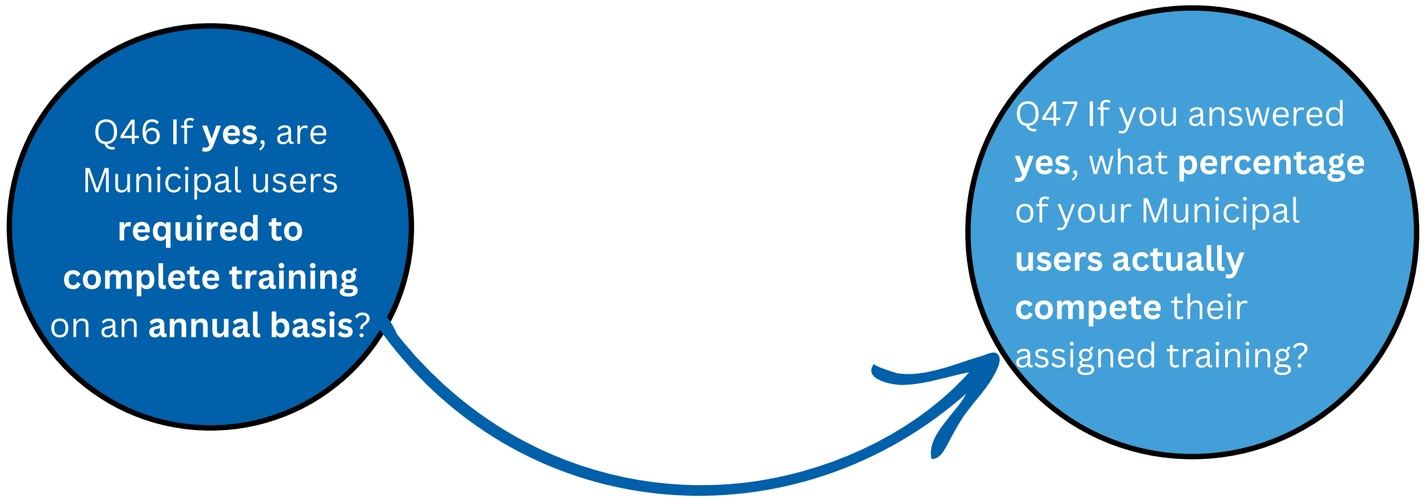
*Q45 If **yes**, **what type** of Municipal users are **part** of the cybersecurity awareness and training program?



*Multiple selections allowed

- **Training participation** recorded:
  - **40% Staff**
  - **21% Management**
  - **36% Elected Officials**
  - **2% Third-party**
- **Noticeable variation** in participation from **2023**:
  - **Third party decreased by 2%**
  - **Elected officials increased by 4%**

Awareness and Training



- **80%** of municipalities **have** made annual trainings **mandatory**
- **10% increase** from 2023
- **More awareness from Governments**

- **53%** municipal users **actually competed** their assigned training
- **Lack of incentive to complete and/or repercussions for not completing**

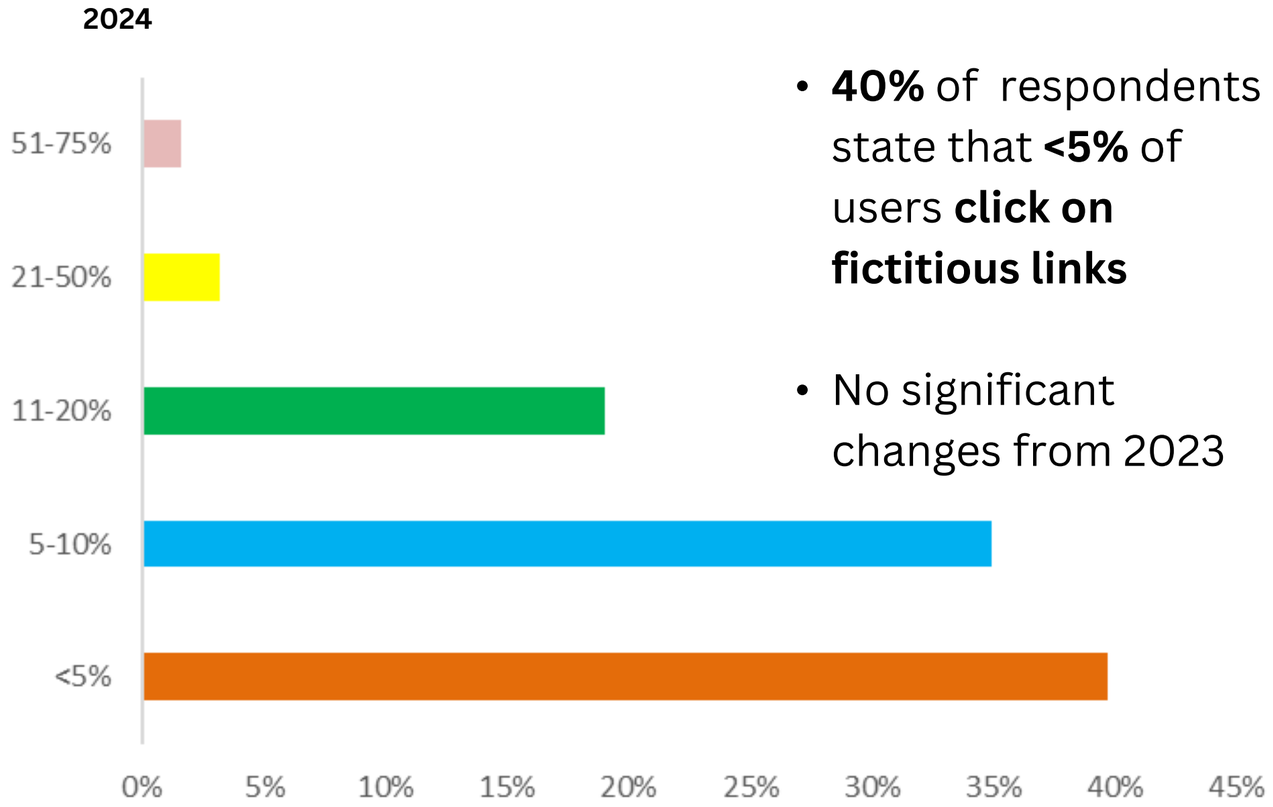
*Questions that show results with less than 10% variation between the 2023 and the 2024 surveys have been grouped together

Awareness and Training

Q48 If **yes**, does your Municipality **conduct Phishing** exercises?

Q49 If you answered **yes**, what **percentage** on average do your Municipal users **click on fictitious links** sent via the Phishing campaign?

- **91%** of municipalities conduct **Phishing** exercises
- **Increase of 20% from 2023**



- **40%** of respondents state that **<5%** of users **click on fictitious links**
- No significant changes from 2023

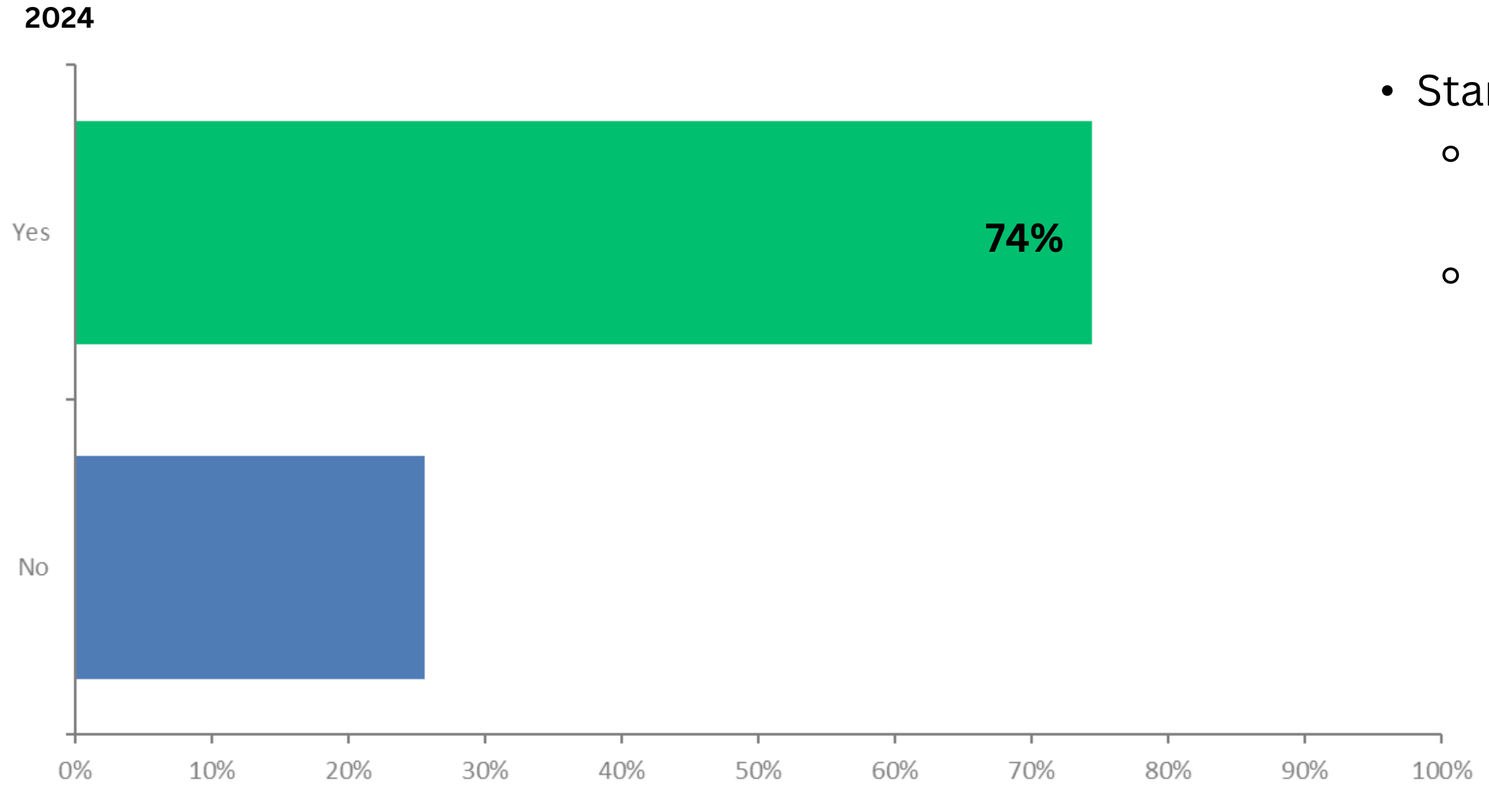
*Questions that show results with less than 10% variation between the 2023 and the 2024 surveys have been grouped together

SECTION 10: ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence (AI)

NEW

Q50 Do you **believe AI** technologies are a **competitive advantage** for Municipalities?



- **74%** of municipalities **believe** AI technologies are a competitive advantage

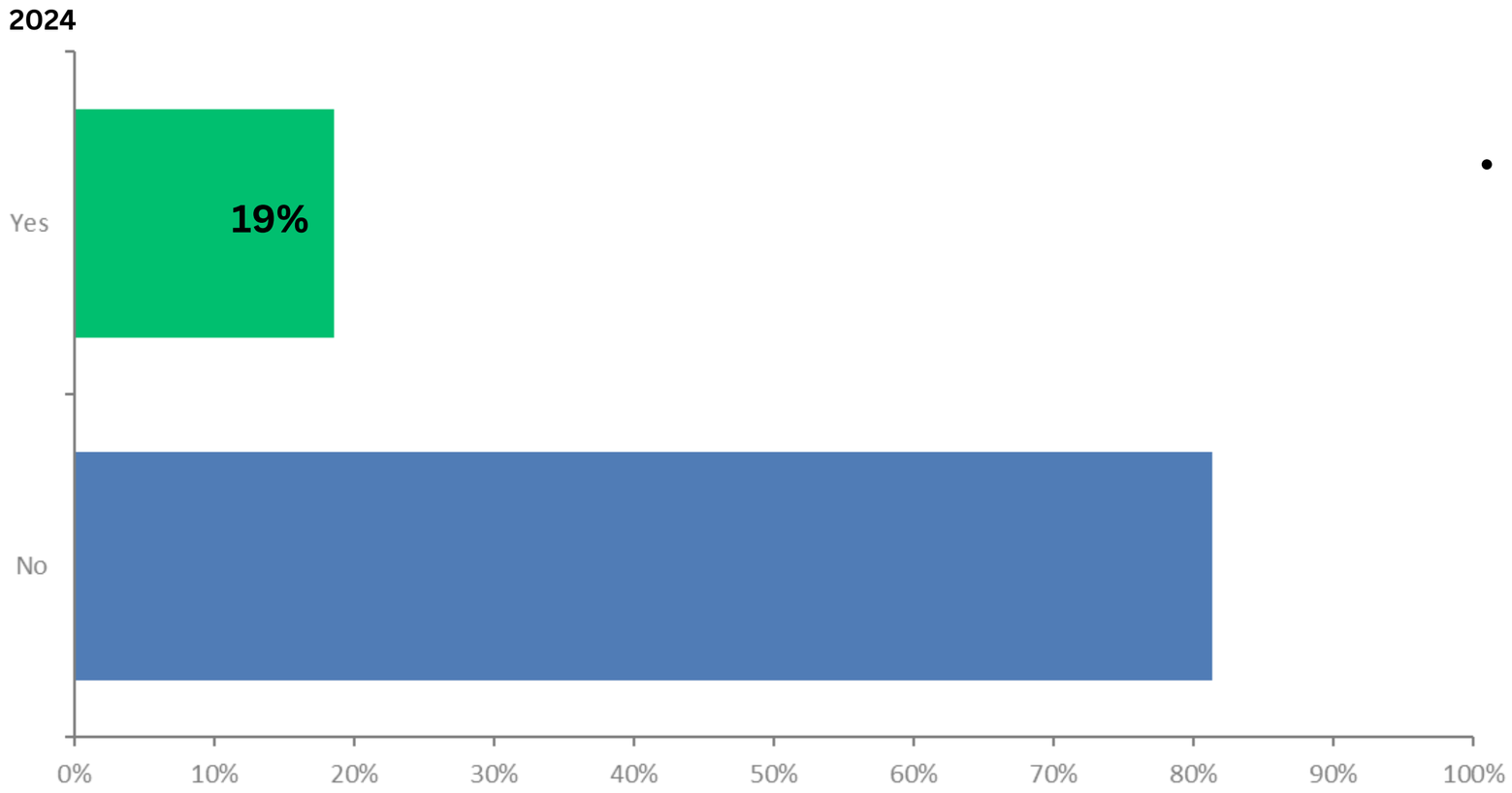
- Started journey:
  - Developed **guidelines and policies**

  - **Deploying AI technologies**
    - Chatbots
    - Transportation
    - Solid waste
    - Homelessness
    - Water demand
    - Council reports
    - Financial fraud
    - Security
    - MS Co-pilot (GenAI – general support)
    - Email filtering
    - Image creation (clipart)

Artificial Intelligence (AI)

NEW

Q51 Has your Municipality **established any** form of **AI Governance** (e.g., policy, framework, guidelines)?

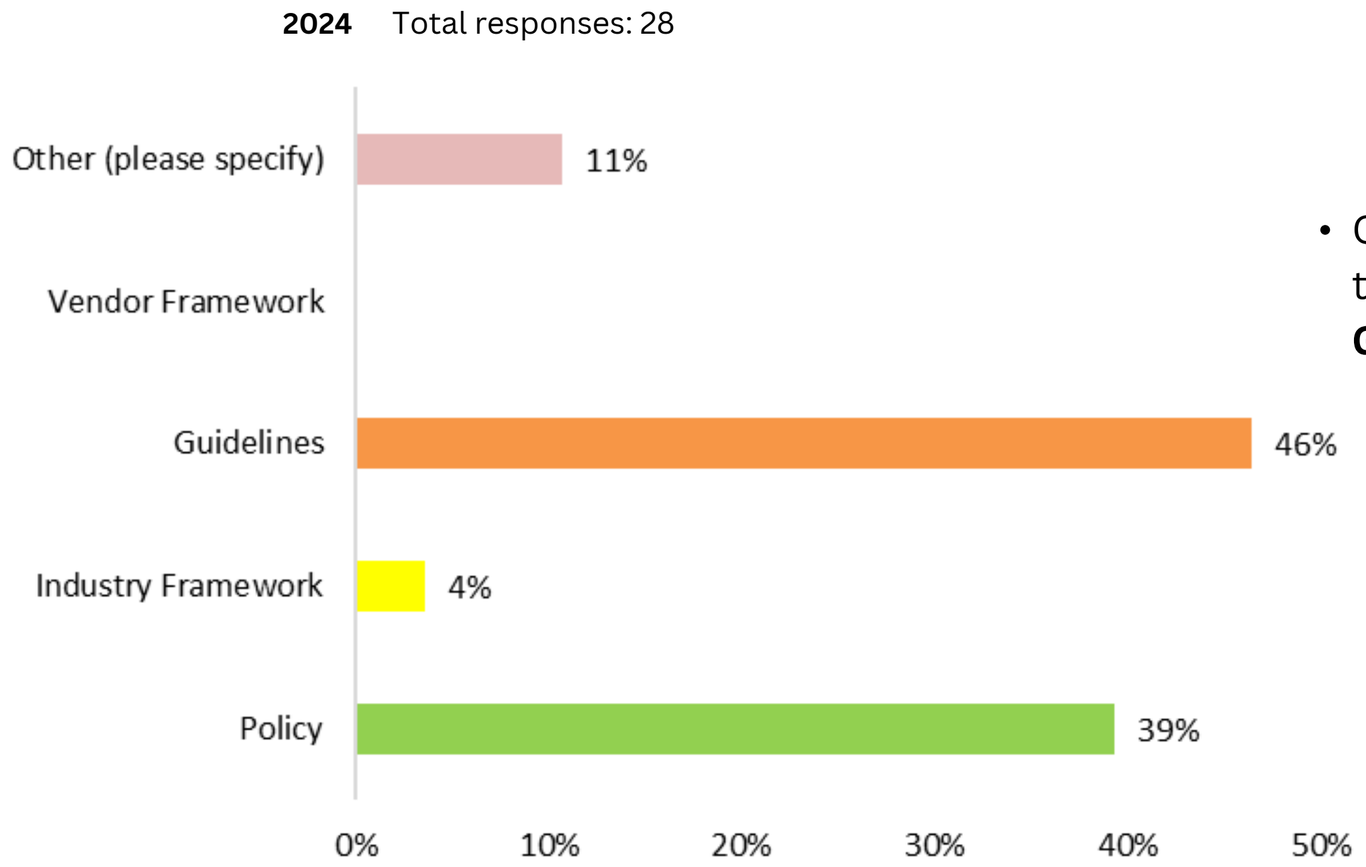


- **19%** of municipalities **have** established some form of AI Governance

Artificial Intelligence (AI)

NEW

Q52 If **yes**, what **type** of AI Governance was established? (Select all that apply)



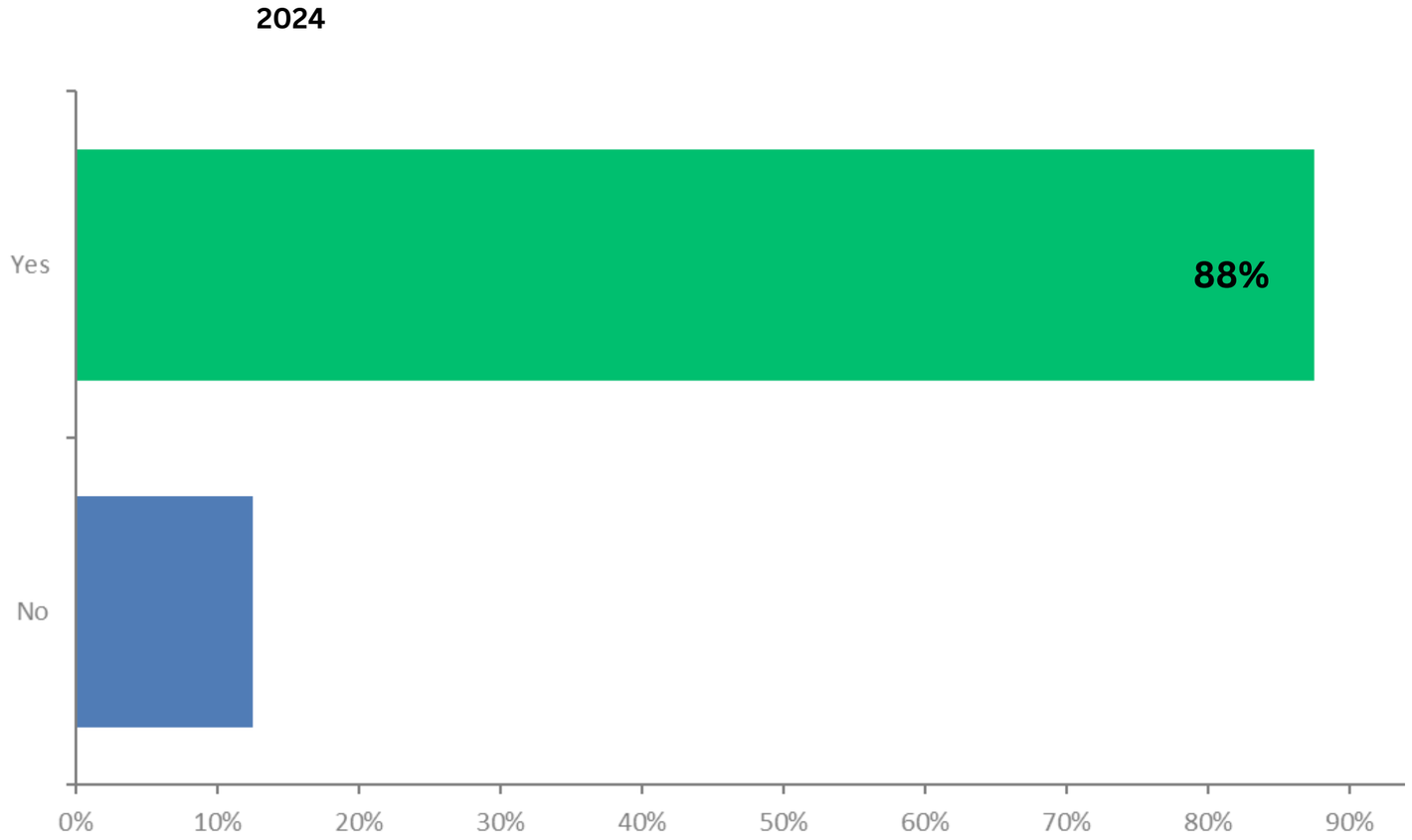
- Of municipalities that **established AI Governance:**
  - **46% have** established **AI Guidelines**
  - **39% have** an **AI Policy**

Multiple selections allowed

Artificial Intelligence (AI)

NEW

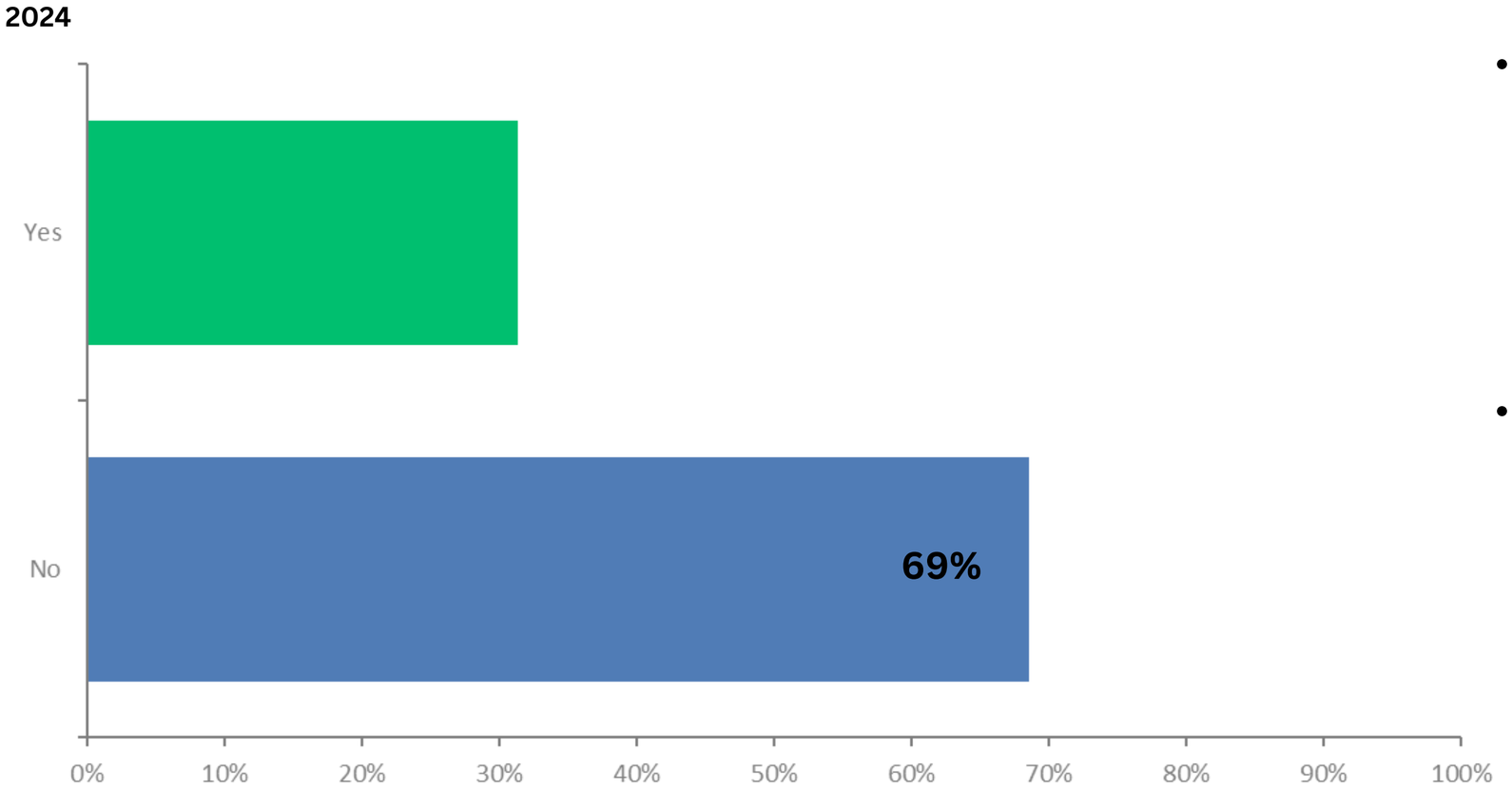
Q53 If **yes**, did your AI **Governance** structure **include cybersecurity**?



- **88%** of municipalities **have included cybersecurity** as part of their AI Governance

Artificial Intelligence (AI)

NEW Q54 Has your Municipality **implemented AI technology**?

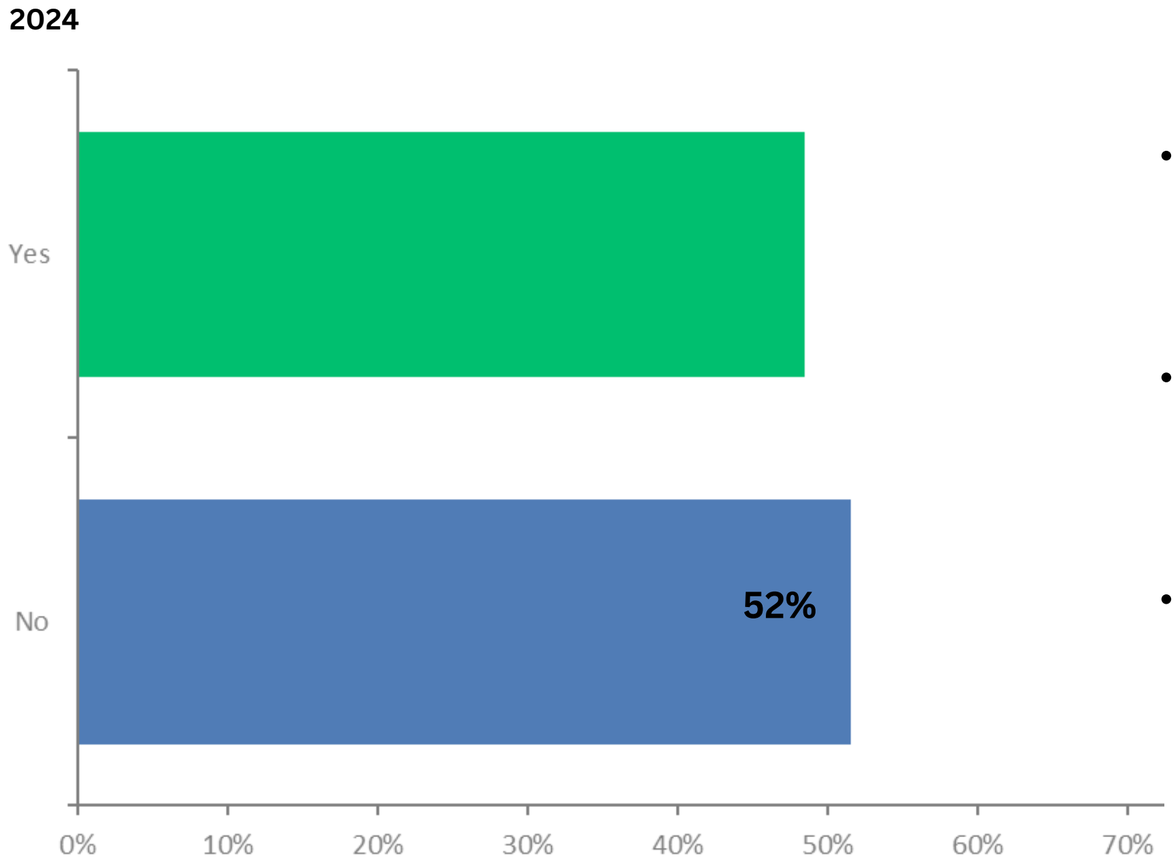


- **69%** of municipalities **have <u>NOT</u>** implemented AI technology
  - Availability of staff resources and skillset
- Implemented AI Tech:
  - Price low
  - Early adoption
  - Shadow AI
  - Train with modern examples

Artificial Intelligence (AI)

NEW

Q56 If **no**, then is your Municipality **considering** implementing AI technology in the **next year**?

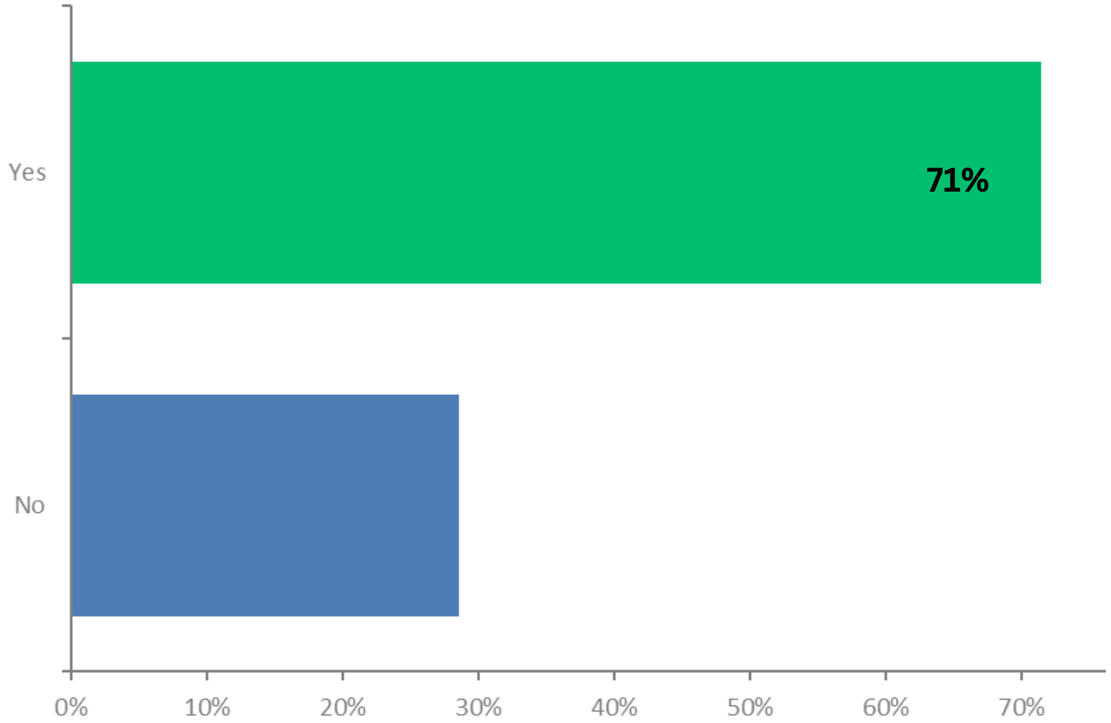


- **52%** municipalities are **NOT considering** implementing AI in **2025**
- **Potential reasons:**
  - **Lack of skillsets**
  - **Lack of resources**
- **Potential Results:**
  - **Loss of competitive advantage**
  - **Loss of efficiency**

Artificial Intelligence (AI)

NEW

Q55 If **yes**, were appropriate **cybersecurity controls** designed/**implemented**?

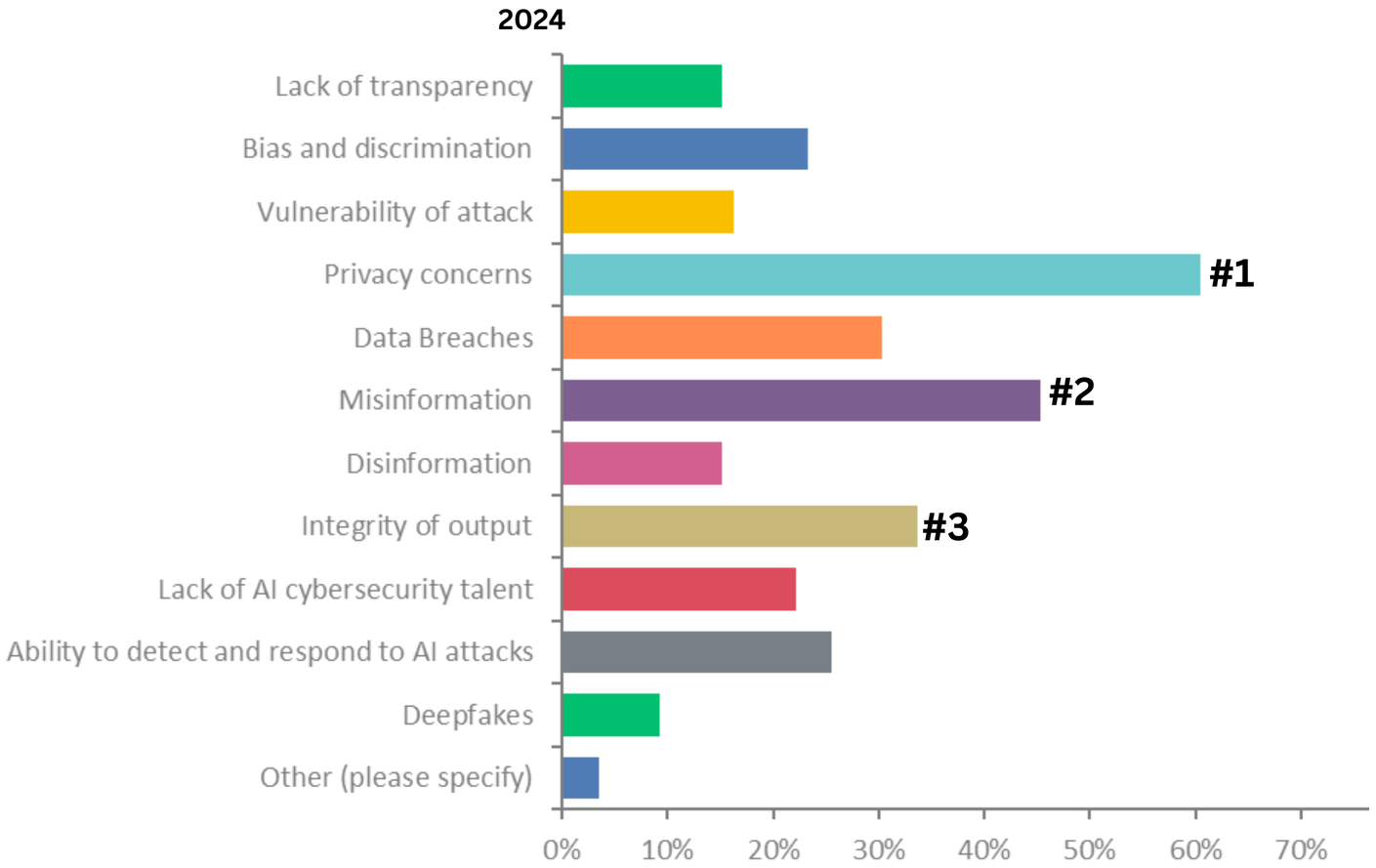


- **71% have** established cybersecurity controls

Artificial Intelligence (AI)

NEW

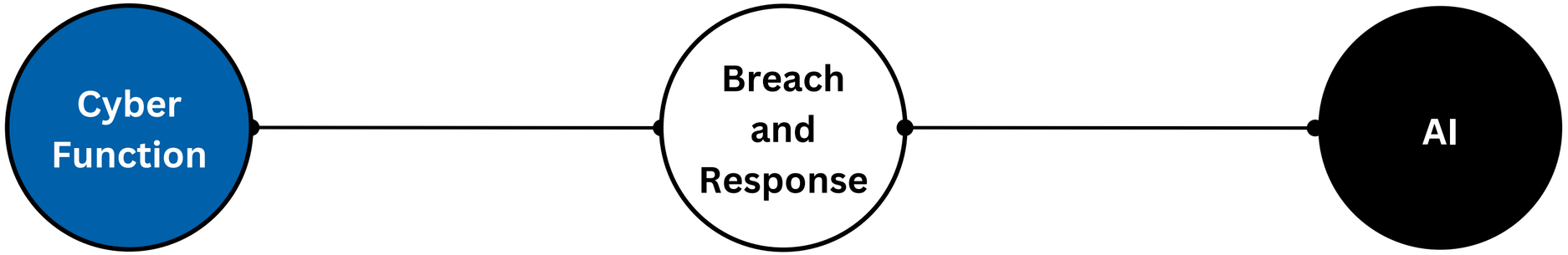
Q57 What are your **top three cybersecurity concerns** regarding the **implementation of AI technologies** in the Municipal sector?



1. **Privacy concerns**
2. **Misinformation**
3. **Integrity of output**

CONCLUSION

2024 Cybersecurity Outlook Survey



- While **tax-based funding** is currently the **norm, more focus:**

- **IT fund reallocation**
- **Partnerships**
- **Cost-sharing** to **reduce reliance on local taxes**

- Municipalities **focusing on:**
  - **Risk tolerance**
  - **Stronger cyber-preparedness**
  - **Cyber operations**

- **To minimize attack impact:**
  - Better leverage **cyber**
  - **Insurance and IR plans**

- Municipalities **are building in security by design principles based on lessons** learnt from **previous technology deployment into AI**

Thank You

Email: info@misa.on.ca | Website: misa.on.ca

Follow us on Twitter, Facebook, and LinkedIn: @misaontario