SECURING THE FUTURE OF URBAN LIVING

Whitepaper

September 2024

GLOBAL CYBERSECURITY FORUM

NEOM نيوم

Foreword

Mesfer Almesfer
Chief Information Security Officer (CISO), NEOM;
Chairman of the Knowledge Community: Securing the Future of Urban Living

As nations shape the cities of tomorrow, cybersecurity has become a critical concern. The promise of cognitive cities and giga-projects holds immense potential but also attracts the attention of cyber adversaries. With vast data volumes and advanced technologies in play, urban environments are prime targets for malicious actors.

Securing our urban future requires a collective effort. That's why our "Securing the Future of Urban Living" Knowledge Community brings together smart city agencies, global cybersecurity organizations, technology companies, think tanks, and academia to address these challenges. Together, we are exploring solutions to create resilient and sustainable cities.

This report presents the key findings from our research, highlighting the cybersecurity challenges and opportunities in cognitive cities. Additionally, members of our Knowledge Community have provided actionable recommendations to enhance urban resilience and protect the future of our digital infrastructure. We extend our sincere thanks to all representatives for their continued dedication to building a secure, sustainable urban future.

Contributors

- **Fahad Al Qahtani,** NEOM, Saudi Arabia
- **Dr. Hussain Aldawood,** NEOM, Saudi Arabia
- **Clay Garner,** SmartCitiesWorld, USA
- **Bruno Lanvin,** Smart City Observatory, Switzerland
- **Dr. Lee McKnight,** Syracuse University, USA
- **Chris Cooke,** SmartCitiesWorld, UK
- **Yusuf Abdul-Qadir,** Syracuse University, USA
- **Samir Aliyev,** Swiss Cyber Institute, Switzerland
- **Daniel González Bootello,** Smart City Cluster, Spain
- **Eduard Dumitrascu,** European Smart Cities Association, Romania
- **Hussain Alebnalshaikh,** University of Wollongong, Australia
- **Dr. Antonio Jara,** Libelium, Spain

Knowledge Community: Securing the Future of Urban Living

We are dedicated to exploring and seizing opportunities to construct a more resilient, sustainable, and equitable urban future. Our strength lies in the diversity of expertise we bring together from multiple stakeholder groups.

The community welcomes smart city agencies, global cybersecurity research organizations, large technology companies, reputable think tanks, academia, and all those with a vested interest in building a secure future.

Contents

Executive summary

This report addresses the evolving landscape of urban environments transitioning from "smart" to "cognitive" cities. Cognitive cities leverage advanced technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) to create more sustainable and responsive urban ecosystems. However, the increased reliance on technology presents significant cybersecurity challenges, with vulnerabilities in communication, edge, and data layers becoming critical areas of concern.

The report is based on a survey of sixty cybersecurity experts across the public, private, and academic sectors, providing valuable insights into cybersecurity preparedness. It identifies a key vulnerability in the communication layer, cited by 40% of respondents as the most vulnerable, followed by the edge layer at 21.7%. The rapid pace of technological change and integration of legacy systems are highlighted as major challenges, emphasizing the need for continuous adaptation of security measures.

Public-private partnerships (PPPs) play a crucial role in addressing these challenges. 30% of respondents pointed to the importance of knowledge sharing between sectors as a vital component of cybersecurity governance. These partnerships help bridge the skills gap, facilitate access to cutting-edge technologies, and foster collaborative frameworks essential for securing cognitive city infrastructures.

Data privacy and ethics are also emphasized, with 63.3% of respondents advocating for stricter access controls and real-time monitoring systems to ensure data integrity. The evolving regulatory landscape presents a mixed outlook, with a need for clearer guidelines and frameworks to address emerging cybersecurity risks.

Key recommendations highlighted in this report, focus on establishing regulatory frameworks that align with international standards, clarifying stakeholder roles, and ensuring policies evolve with technological advancements.

Strengthening public-private partnerships is vital to drive innovation in cybersecurity solutions. Addressing the skills gap through targeted education and training is crucial for developing a workforce capable of managing cognitive city systems.

Additionally, rigorous data privacy measures—such as encryption and regular audits—are essential to protect urban environments. A human-centric approach is critical, involving citizens in policymaking to ensure cybersecurity measures reflect real-world needs.

1. Introduction

As cities develop further into digitally interconnected systems, they have the potential to become more efficient, sustainable, and responsive to the needs of residents.[1]

While smart cities use digital technologies to enhance efficiency and livability, cognitive cities represent a more advanced integration of artificial intelligence and the Internet of Things (IoT), enabling urban environments to learn, adapt and respond to the needs of their inhabitants in real-time. However, this increased technological integration also increases their cyber-attack surface, posing new risks to critical infrastructure, public services, and the privacy and trust of residents, which cognitive cities must manage effectively.[2][3][4][i]

To contribute to the ongoing discourse on urban cybersecurity, we surveyed 60 city-focused practitioners across various regions, sectors, and organizational sizes. This sample size precludes overly broad generalizations and surpasses typical response rates in similar studies, offering valuable insights into cybersecurity readiness in cognitive cities[ii], aiming to illuminate key challenges and opportunities and provide a basis for further research and policy discussions.

Figures 1, 2, and 3 show that the 60 survey respondents were a balanced sample from the public sector, private sector and academia/NGOs worldwide. Data was collected from April to May 2024.

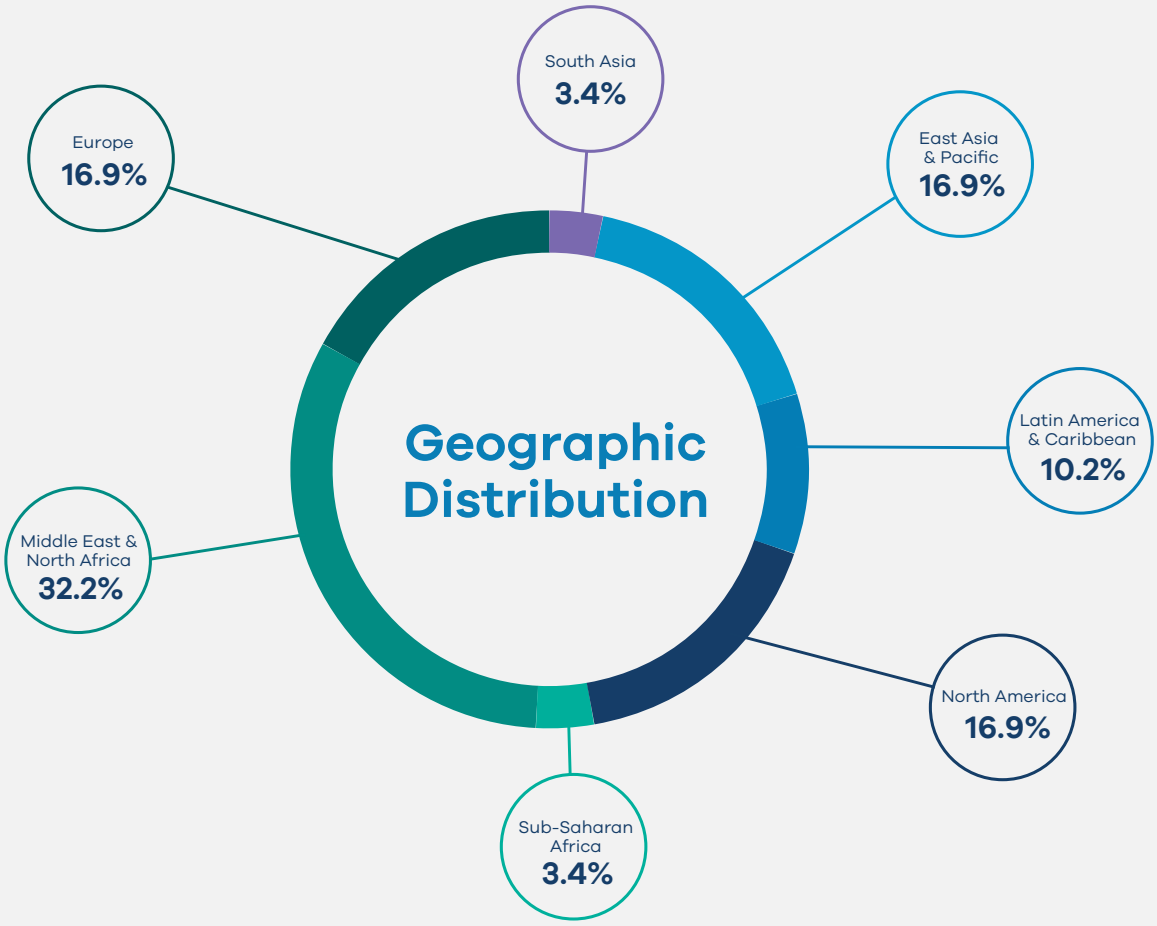


Figure 1: Geographic distribution of respondents' headquarters

[i] Smart cities enhance and streamline city operations using IoT and data, while cognitive cities represent the next step, integrating AI and advanced analytics to enable proactive and intelligent decision-making.
[ii] In Aldawood and Skinner (2020), the semi-structured survey had 21 respondents, which is already more than 10-20 on average seen in this type of paper. Ours had 60.

Figure 2: Category best describing organization's primary focus

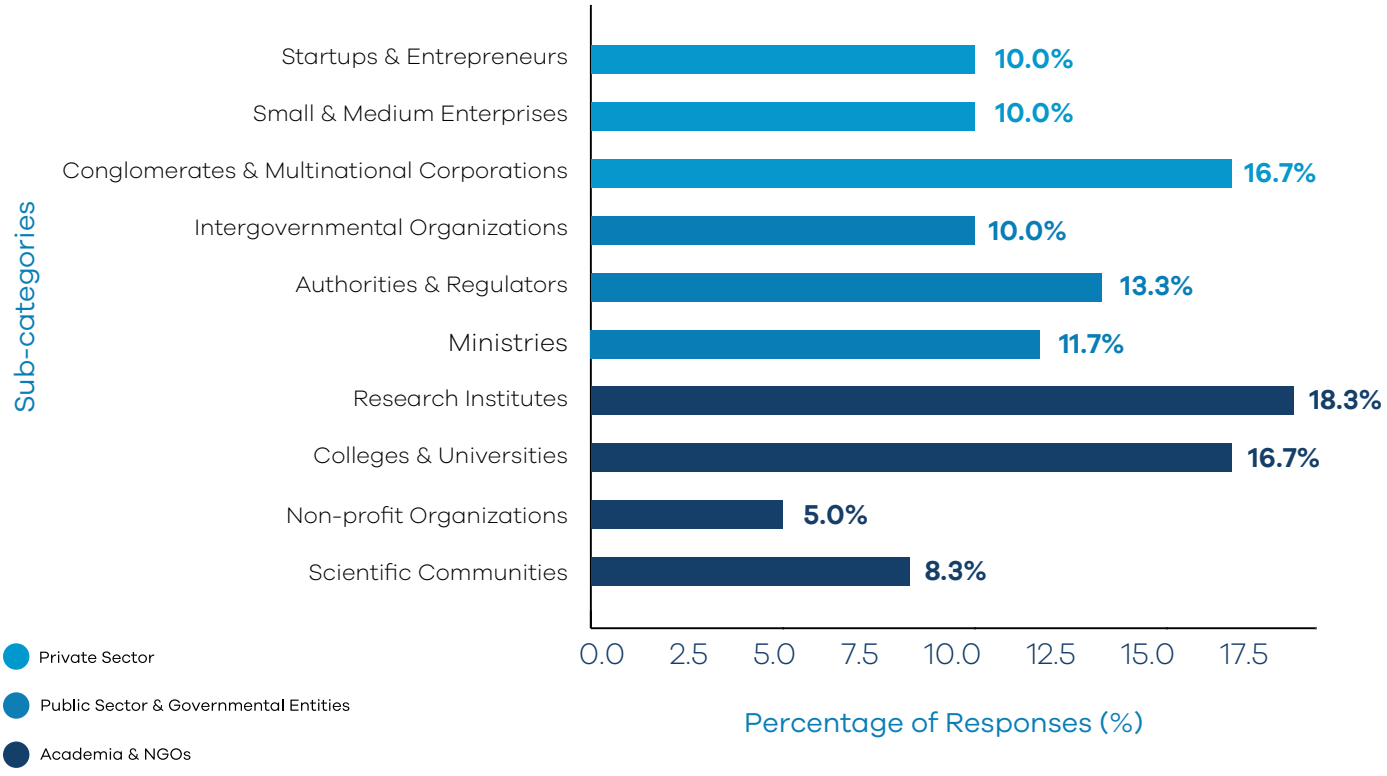


Figure 3: Organization types for survey respondents

2. Survey Insights: Challenges and Opportunities in Securing the Future of Urban Living

As urban areas evolve into cognitive cities, they face complex cybersecurity challenges that underscore the need for strategic adaptation and robust security measures.

Our survey insights reveal a critical vulnerability in the communication and edge layers of urban infrastructure, areas integral to the operation and data management of cognitive cities. These vulnerabilities require a proactive approach to cybersecurity, focusing on rigorous security protocols and innovative solutions to protect these fundamental components from cyber threats.

To address these vulnerabilities, our respondents emphasize the importance of a collaborative approach to governance and risk management that involves both the public and private sectors. This approach involves sharing expertise and resources to foster innovative cybersecurity solutions, ensuring access to cutting-edge technology, and setting up comprehensive governance frameworks.

Such collaboration is vital for maintaining data integrity and privacy, as highlighted by strict access controls, real-time monitoring and regular security audits. Moreover, navigating the complex regulatory landscape remains a formidable challenge, with a pressing need for clear standards and effective public-private partnerships to bridge the skills gap and advance the secure development of cognitive cities.

2.1 Vulnerability Landscape

LAYER	DESCRIPTION
Communication Layer	Secures data transmission between devices and central systems to prevent interception and tampering.
Core Layer	Protects central infrastructure (e.g., servers and data centers) from attacks, ensuring data integrity and service availability.
Edge Layer	Secures peripheral devices (e.g., sensors and cameras) from physical tampering and unauthorized access.
Data Layer	Protects stored data from breaches, ensuring privacy and integrity through encryption and access controls.
API Layer	Secures software interfaces to prevent unauthorized access and common vulnerabilities.
Enabler Layer	Ensures the security and reliability of supporting technologies, such as cloud services and identity management systems.

Figure 4: Description of cybersecurity measures by layer

The survey results show that 40% of respondents consider the communication layer the most vulnerable part of smart/ cognitive city systems, closely followed by the edge layer (21.7%).

This figure is significant and underscores the critical nature of this layer, which serves as the backbone for data transmission. The fact that the primary threats to this layer are cyberattacks (51.7%) and data interception (30%) highlights a pressing need for robust security protocols.

The emergence of new regulations, such as the Networks and Information Systems Directive (NIS2) in Europe and the Cyber Resilience Act (CRA), are reflected in the priorities of respondents. These practices define a new cybersecurity paradigm for critical infrastructure, including in waste management, water management, mobility and other domains relevant to cognitive cities.[5]

The respondents' focus on connectivity and edge cybersecurity reflects the key roles of wireless communications and digital transformation efforts that rely on more connected infrastructures. It is also noteworthy that cloud security, much discussed in the media, is not a top concern of these practitioners. A secure cloud architecture for smart cities can be part of the solution for future cognitive cities to monitor and manage the diversity of edge (cyber-physical) systems proliferating across communities.

21.7% of respondents perceive the edge layer as highly vulnerable, threatened primarily by unauthorized access or hacking (55%).

This layer, consisting of devices at the 'edge' of the city's network — like surveillance cameras and traffic sensors — is crucial for gathering and processing data locally, especially for applying advanced AI models requiring high performance and low latency.

Saving costs on bandwidth while promoting privacy and compliance with globally adopted regulations, such as GDPR, is challenging. Therefore, edge computing is considered a vulnerable domain due to its remote and distributed allocation and its proliferation of billions of devices across communities, which provides cyber-threat actors with countless soft targets. It is also an opportunity to improve cognitive city performance due to the new capabilities to protect, aggregate, anonymize and minimize data exposition.

The prevalence of unauthorized access concerns suggests a vulnerability to exploitation that could compromise the entire city network in the worst case or myriad specific services and devices in more limited intrusion scenarios. This vulnerability is exacerbated by technological complexity and difficulties integrating with legacy systems (31.7%), which can hinder timely updates and security patch implementations.

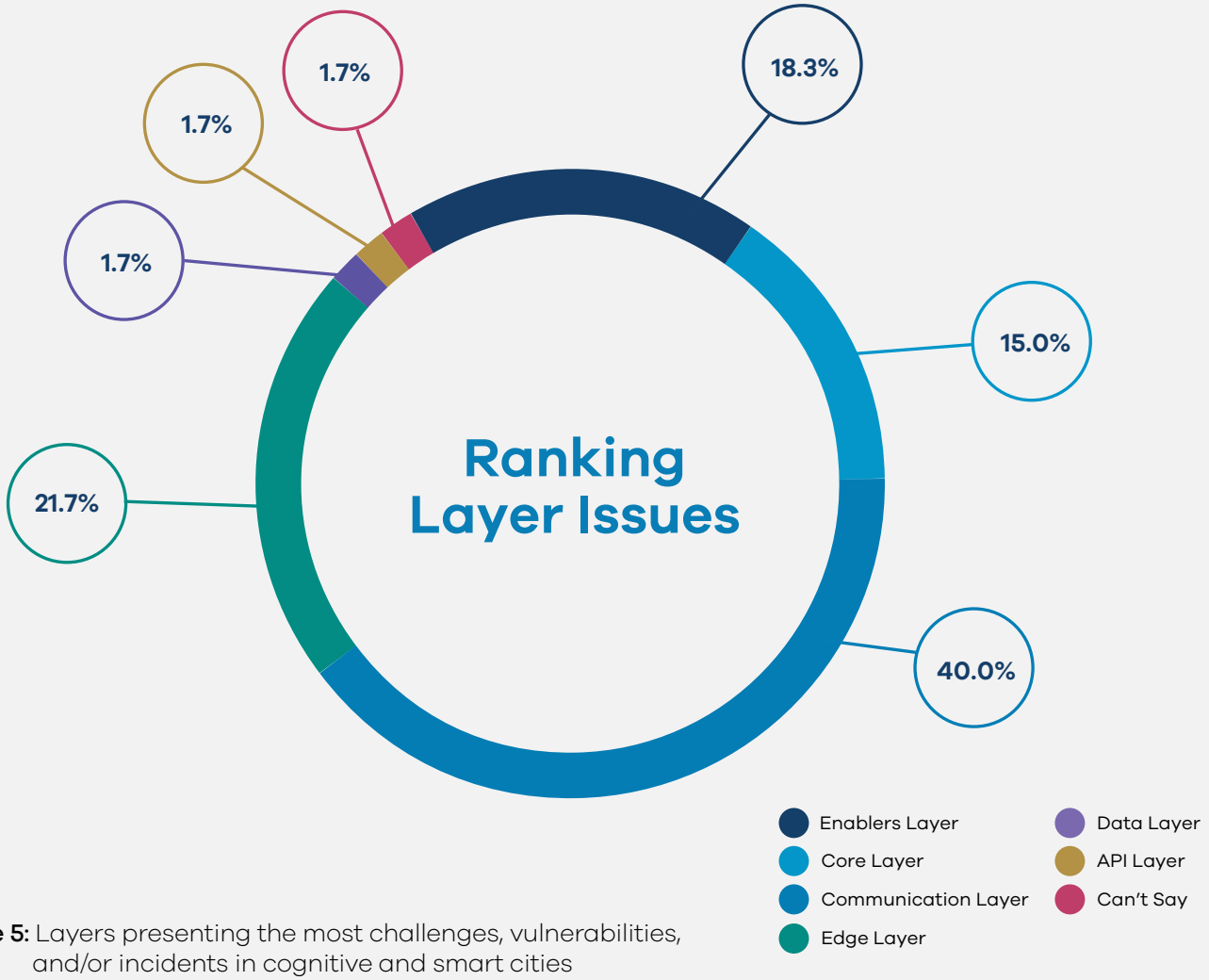


Figure 5: Layers presenting the most challenges, vulnerabilities, and/or incidents in cognitive and smart cities

Most respondents (60%) named the complexity of coordinating between diverse service providers and vendors as a major challenge in managing the communication layer.

Low-power communications network technologies for the Internet of Things (IoT), such as LoRa (Long Range), SigFox, and other Low Power Wide Area Networks (LPWANs), are often battery-powered. This presents limitations in terms of advanced cybersecurity capabilities and high vulnerability for DDoS (Distributed Denial of Service) attacks.

Consequently, there is also a strong focus on the benefits of cellular communications, such as NB-IoT, and new protocols for IoT, including Ultra-High Reliability and Low Latency (URLLC) protocols that aim to address these challenges with the support of the base stations as edge infrastructure; albeit with cost trade-offs. Therefore, their reliability and cybersecurity capabilities will be key performance factors for deciding between different future communications mediums.

Moreover, 58.3% of respondents emphasized the difficulty for their organizations in keeping pace with rapid technological changes, requiring specialized knowledge, training, and skills. The core layer faces similar challenges, with 65% of respondents highlighting the need to keep pace with swift technological advancements.

This underscores the importance of continuous updates and adaptability in cybersecurity measures, including training, education and staff cybersecurity awareness. Key protocols for Smart Cities such as OMA LwM2M for Device Management are increasingly relevant, as their capabilities for upgradeability, maintenance and their adaptive orientation to address cybersecurity and communication requirements over time are key benefits also for future Cognitive Cities.[iii]

For the core layer, enhancing monitoring and response capabilities is seen as crucial by 71.7% of respondents, while disaster recovery capabilities are emphasized by 66.7%. These priorities indicate the importance of being prepared for and resilient to cyber threats. Additionally, the seamless integration of IT (Information Technology) and operational technology (OT) systems is considered essential by 60% of respondents. Operational technology includes traditional SCADA (Supervisory Control and Data Acquisition) networks and the broader field of advanced cyber-physical systems and Industrial IoT services critical for Industry 4.0 applications.[iv]

[iii] OMA Lightweight M2M (LwM2M) is an open protocol from the Open Mobile Alliance (OMA) that manages devices and enables services for the Internet of Things (IoT) or machine to machine (M2M). It was designed to meet the needs of mobile devices with limited compute power and limited battery power.
[iv] See Sathyan Munirathinam, Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT), in Pethuru Raj, Preetha Evangeline, Eds., Advances in Computers, Elsevier, Volume 117, Issue 1, 2020, pp. 129-164, ISSN 0065-2458,ISBN 9780128187562, https://doi.org/10.1016/bs.adcom.2019.10.010. (https://www.sciencedirect.com/science/article/pii/S0065245819300634)

2.2 The Role of Public-Private Partnerships in Governance and Capacity-Building

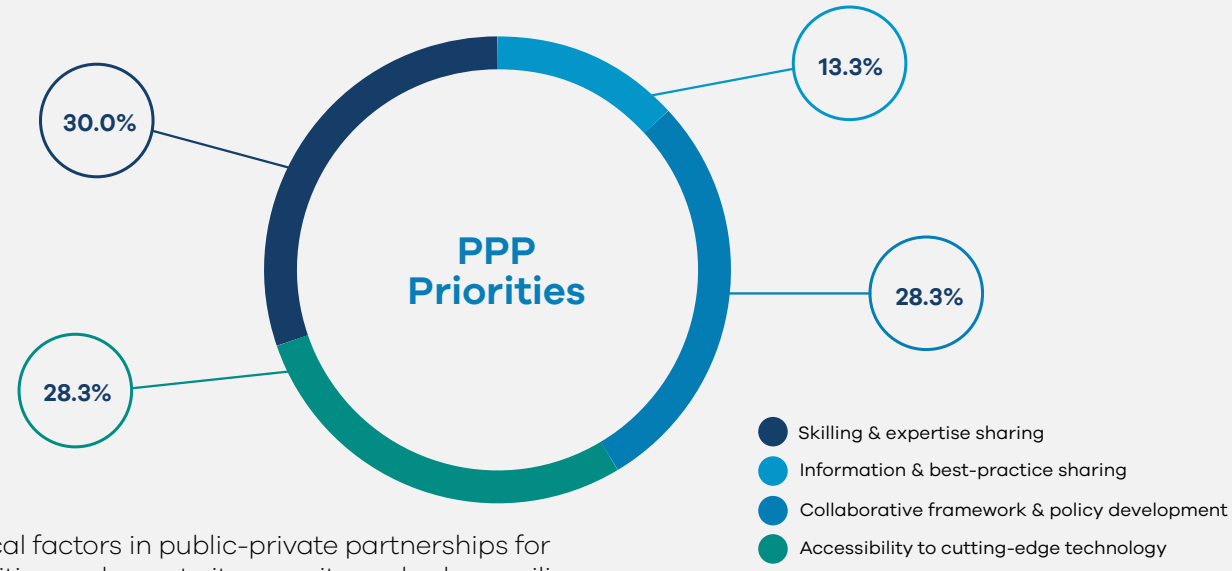


Figure 6: Critical factors in public-private partnerships for cognitive and smart city security and cyber resilience

In exploring the impact of multisector collaboration on cybersecurity governance and capacity-building, our survey asked participants to identify key factors critical to the success of public-private partnerships.

For 30% of respondents, the foremost components for success in public-private partnerships are skill and expertise sharing.

This emphasis underscores the benefits of harnessing diverse knowledge and experience from the public and private sectors to craft effective cybersecurity strategies. Through such partnerships, cities access private sector technical skills and innovative approaches, while private entities gain an understanding of urban challenges, regulatory environments, and barriers to innovation. This reciprocal knowledge exchange is essential for constructing adaptive cybersecurity frameworks capable of responding to the dynamic threats that cognitive cities encounter.

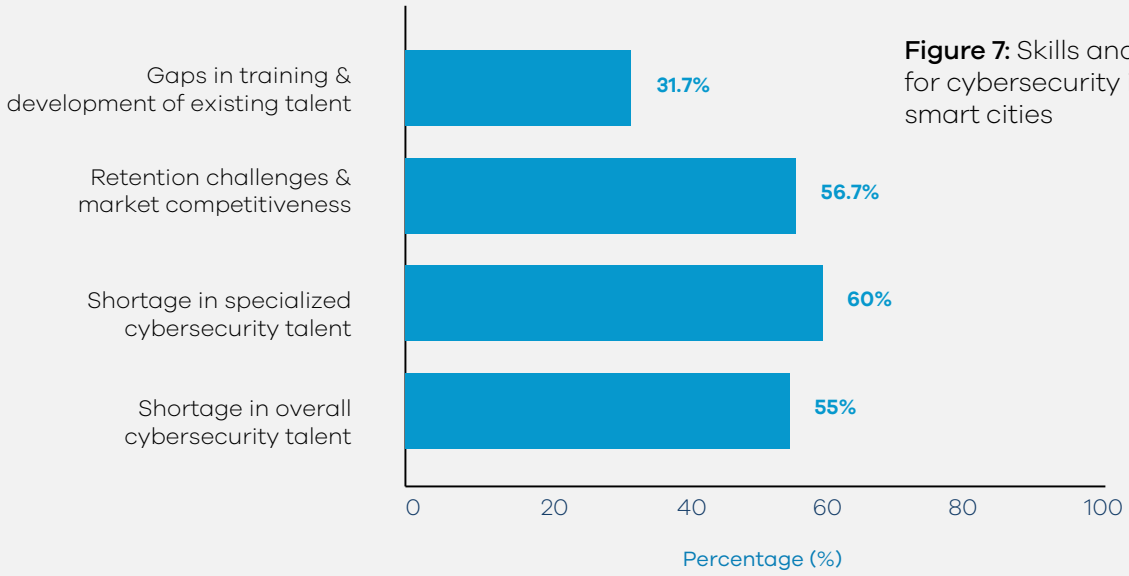


Figure 7: Skills and talent gap for cybersecurity in cognitive/ smart cities

The survey reveals a critical skills and talent gap across cognitive cities, acknowledged by 100% of respondents, emphasizing the pressing need for a robust cybersecurity workforce.

Specifically, 60% reported a severe shortage of specialized cybersecurity professionals, underscoring the urgent need for targeted educational and training programs.

Furthermore, 56.7% identified retention challenges exacerbated by a competitive market, highlighting the dual challenge of attracting and retaining top talent in the cybersecurity sector, contributing to the 55% shortfall.

To address these issues, 31.7% of respondents pointed out significant gaps in the training and development of existing talent. This situation calls for a dual approach to workforce development: enhancing recruitment strategies to attract skilled professionals and investing in continuous professional development to keep them.

A comprehensive strategy integrating practical experience with theoretical knowledge is essential, potentially through partnerships with academic institutions and industry leaders, to ensure the curriculum remains relevant and innovative. Such a comprehensive approach is crucial for developing a resilient cybersecurity workforce to safeguard urban infrastructures against sophisticated threats.

In parallel, 28.3% of respondents highlighted the critical importance of accessing cutting-edge technology.

Cognitive cities, dependent on advanced technological infrastructure, require the latest tools and solutions for effective cybersecurity.

Public-private partnerships are vital in facilitating access to these technologies, enabling cities to deploy state-of-the-art systems that enhance their capability to detect, prevent, and respond to cyber threats. This access bolsters security and drives innovation as public and private sectors collaborate to develop new solutions tailored to the unique needs of urban environments.

Similarly, another 28.3% of participants stressed the need for developing collaborative frameworks and policies. Establishing clear guidelines and protocols for cooperation between public and private entities is critical for ensuring a cohesive and coordinated cybersecurity effort. These frameworks help define roles and responsibilities, streamline communication, and standardize incident response and information-sharing procedures. By fostering a well-defined collaborative environment, public and private partners can significantly enhance their collective ability to protect the digital infrastructures of urban areas.

“Cognitive cities, dependent on advanced technological infrastructure, require the latest tools and solutions for effective cybersecurity.”

2.3 Data Privacy, Trust, and Ethics

Ensuring the privacy and integrity of data collected by edge devices is a key concern for the future of urban cybersecurity.

As cities evolve into cognitive environments, the volume and sensitivity of data increases, necessitating robust strategies to protect this information. On the other hand, some city data may be shared openly, as reflected in the growth of open data portals for citizens and others to assess and make their own analytical contributions.[v] As a result, data risk classification is also needed in cognitive cities so that only the most sensitive data is subject to the strictest and most costly data controls.[6] Our survey highlights several approaches perceived as most effective in ensuring data privacy and integrity.

Moreover, the pervasive 'datafication' within smart cities presents significant ethical challenges.[7] NIST (National Institute of Standards and Technology) recently developed an approach to encouraging communities to create their own holistic key performance indicators (H-KPIs), described in "Smart Cities and Communities: A Key Performance Indicators Framework," which is one way for cities to manage these challenges.[8]

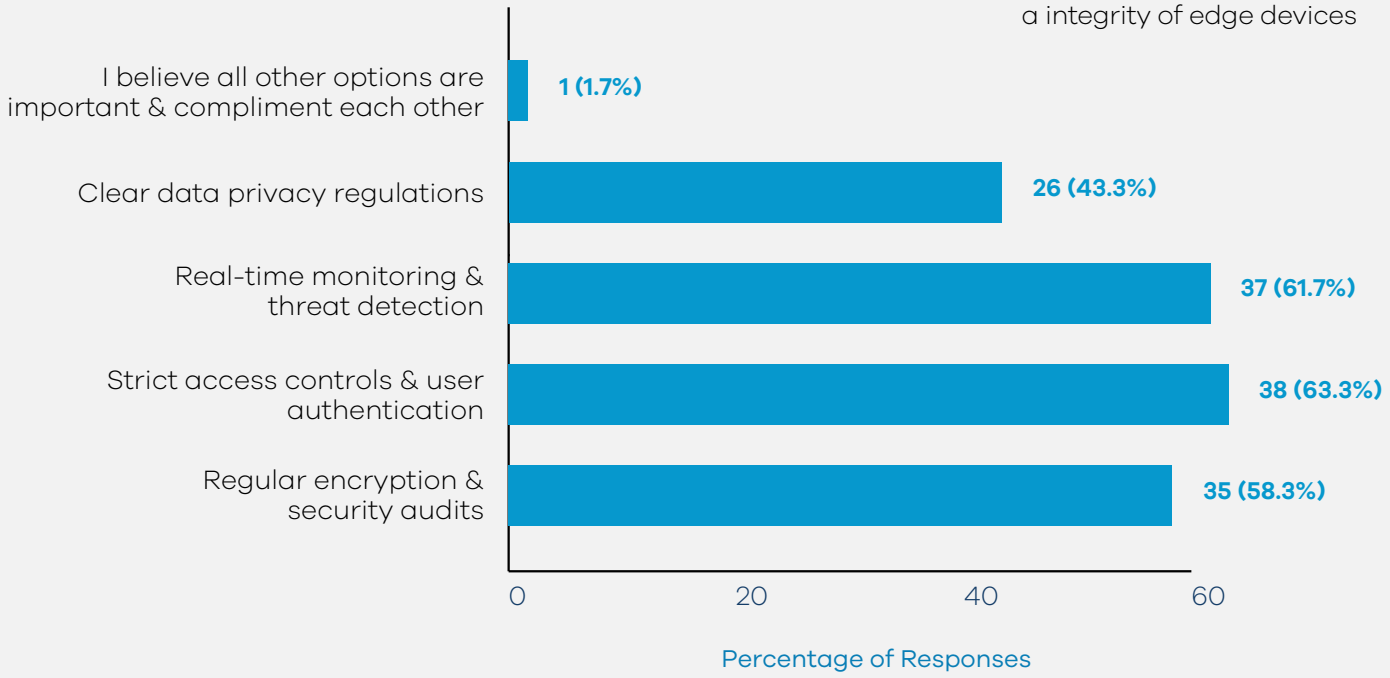
NIST states: "The H-KPI method provides a structured representation of smart city/community information flows that supports system visualization, serves as the basis for quantitative metrics for measuring 'smart,' and enables computational methods for systems design, analysis, operations, and assurance. The five core metrics of the method are the alignment of KPIs with community priorities across districts and neighborhoods; investment alignment with community priorities; investment efficiency; information flow density; and quality of infrastructure services and community benefits."

"As cities evolve into cognitive environments, the volume and sensitivity of data increases, necessitating robust strategies to protect this information."

[v] See for example City of Syracuse (New York, U.S.A.) Open Data Portal https://data.syr.gov/

The survey responses show that strict access controls and user authentication, real-time monitoring and threat detection, and regular encryption and security audits are viewed as the most critical methods for ensuring the privacy and integrity of data collected by edge devices.

Figure 8: Effectiveness of approaches to data privacy a integrity of edge devices



Strict Access Controls and User Authentication: Most respondents (63.3%) emphasized the importance of implementing strict role-based access controls and user authentication mechanisms. These measures are crucial in preventing unauthorized access to sensitive data and ensuring that only authorized individuals can interact with critical systems. By verifying the identity of users and restricting access based on roles and permissions, cities can significantly reduce the risk of data breaches.

Real-Time Monitoring and Threat Detection: Real-time monitoring and threat detection are seen by a majority of respondents (61.7%) as vital for providing immediate responses to potential security threats. This approach involves continuously observing network activity, identifying unusual patterns, and promptly addressing anomalies that could indicate a security breach.

Implementing real-time monitoring systems helps cities quickly detect and mitigate cyber threats before they can cause significant harm. Machine learning and artificial intelligence capabilities may significantly improve these capabilities in the future. Still, cyber-threat actors will also use them to detect vulnerabilities and further automate system breaches.

Regular Encryption and Security Audits:
While slightly less prioritized than access controls and real-time monitoring, most respondents (58.3%) still deem regular encryption and security audits essential. Encryption ensures that data remains protected even if intercepted, rendering it unreadable to unauthorized users. On the other hand, security audits involve systematically evaluating security measures to identify vulnerabilities and ensure compliance with established protocols and regulatory requirements. Together, these practices contribute to a robust defense against data breaches and cyberattacks.

In addition to technical measures, clear data privacy regulations are also considered important, with 43.3% of respondents highlighting their significance. These regulations provide a legal framework that governs the collection, storage and use of data, particularly personally identifiable data, ensuring that privacy rights are upheld and that organizations are held accountable for protecting sensitive information.

The European General Data Data Protection Regulation, or GDPR, is the best-known example, although it is not without its critics regarding its effectiveness in practice. The GDPR applies to companies of all sizes and across sectors, regardless of location, if they process the personal data of anyone in the EU. By establishing and enforcing clear data privacy policies, cities can build trust with residents and stakeholders, demonstrating their commitment to safeguarding personal information.

2.4 Navigating Regulatory Landscapes

Managing the complexities of technology risk poses a significant regulatory challenge for emerging cognitive cities.

According to 51.7% of survey respondents, the primary difficulty lies in understanding, integrating and regulating new technologies. The rapid pace of technological change often outstrips the ability of regulatory frameworks to adapt, creating governance gaps that can be exploited. Furthermore, 23.3% of respondents highlighted the tension between fostering innovation and maintaining regulatory compliance. This balance is crucial: while innovation drives urban progress and enhances the quality of life, it must be pursued within a framework that ensures security and protects public interests. Striking this balance is a central challenge for policymakers in the context of cognitive cities.

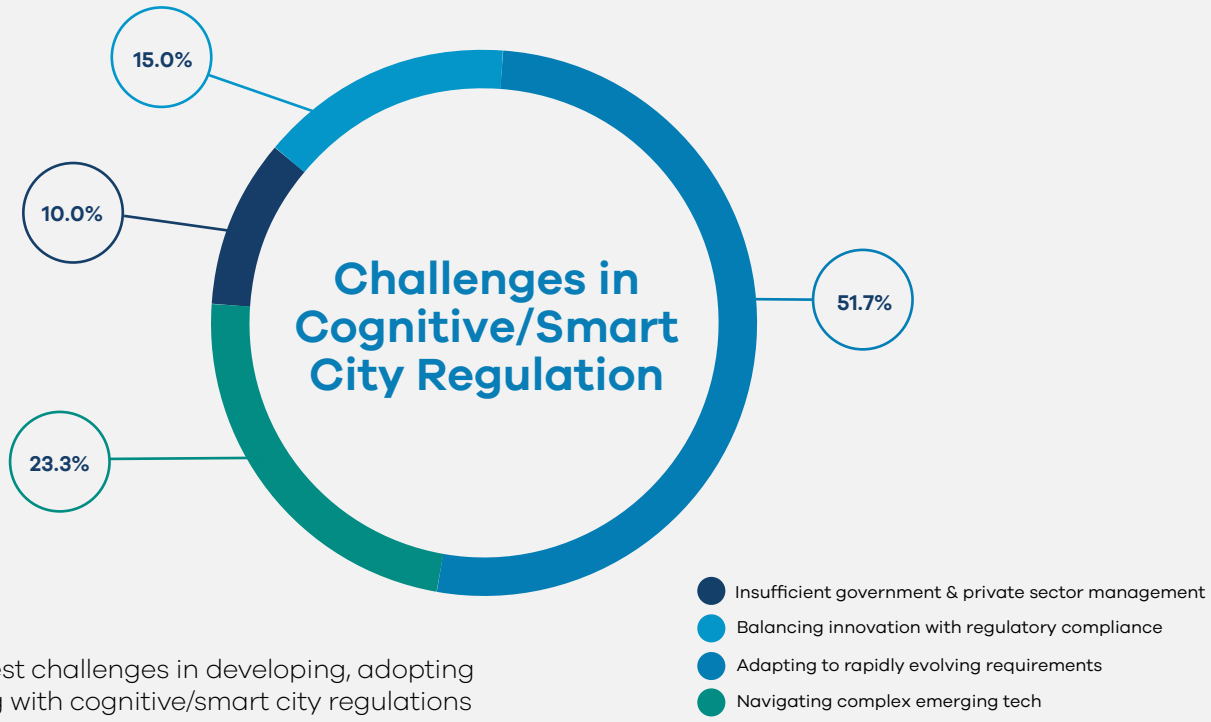


Figure 9: Biggest challenges in developing, adopting and complying with cognitive/smart city regulations

The survey responses show varying perceptions of the adequacy of current regulations in safeguarding cognitive city projects:

- **Moderately Adequate:** A majority of respondents (58.3%) believe that existing regulations provide a basic level of security. This suggests that while current regulations are helpful, they are insufficient to address the rapidly evolving cybersecurity threats specific to cognitive cities.
- **Very Adequate:** A significant number of respondents (30%) feel confident that current regulations are sufficient to ensure security, indicating satisfaction with existing compliance measures.
- **Not Adequate:** About 11.7% consider the current regulations inadequate, implying that security can only be ensured through additional efforts beyond compliance with existing standards.

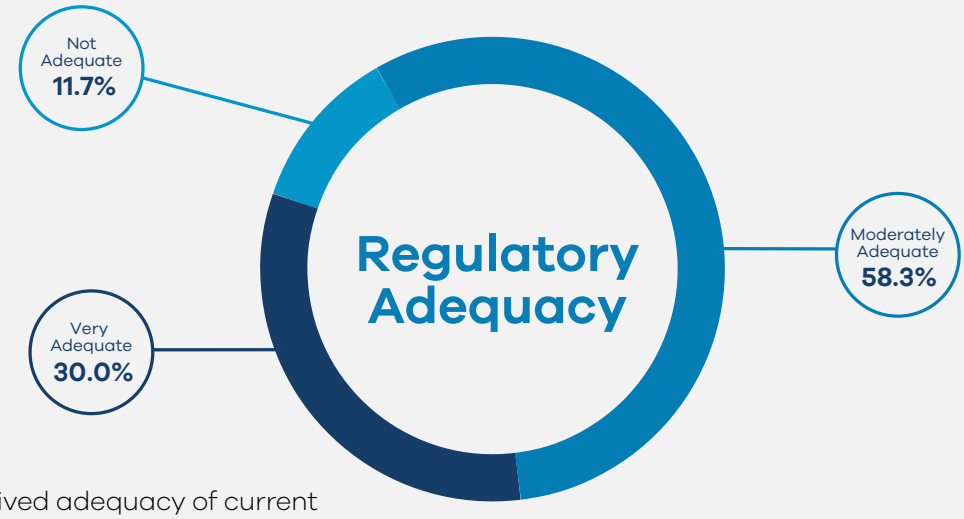


Figure 10: Perceived adequacy of current regulations in safeguarding cognitive city projects

Respondents identified several key areas for improvement to enhance the regulatory landscape and better secure cognitive cities.

First, 41.7% of respondents highlighted clarifying standards and guidelines. They emphasized the need for clear and detailed regulatory frameworks to ensure that all stakeholders understand their obligations and collaborate more effectively to secure urban technologies. Preis and Susskind (2022) underscore this necessity by highlighting the fragmented nature of local governance and the critical need for coordinated cybersecurity strategies.[9]

Second, 26.7% of respondents deemed building public-private partnerships essential. They noted that collaboration between the public and private sectors could leverage their expertise and resources, leading to innovative solutions and robust cybersecurity measures. Enhanced cooperation would also facilitate better communication and more cohesive management of urban cybersecurity.

Third, 18.3% of respondents identified bridging the skills gap as a critical area. Addressing the shortage of specialized cybersecurity talent requires increasing staff awareness and providing targeted training and development programs. This would help build a competent workforce capable of managing the sophisticated cybersecurity needs of cognitive cities.

Finally, 13.3% of respondents mentioned enhancing regulatory frameworks. For instance, aligning a city's posture with international standards such as the GDPR or NIS Directive can provide a robust baseline for data protection and cybersecurity and be further tailored to address the specific needs of cognitive cities. While less emphasized, updating and refining existing regulations remains important to keep pace with technological advancements and emerging threats, ensuring they stay relevant and effective.

3. Recommendations for Stakeholders

Our recommendations are informed by the authors' collective insights and expertise, further enriched by the survey results. They are designed to guide stakeholders in enhancing the cybersecurity resilience and readiness of cognitive cities.

3.1 Regulation

Developing comprehensive guidelines delineating roles and responsibilities is pivotal for maintaining cybersecurity and building resilience.

Regular updates to these regulatory frameworks are crucial to accommodate technological progress and evolving cyber threats. Survey insights indicate that 41.7% of respondents believe clarifying standards and guidelines is critical, underscoring the necessity of a dynamic regulatory environment that adapts quickly to new challenges. The following points summarize our recommendations on regulation:

- Develop and benchmark a comprehensive set of cybersecurity metrics by leveraging a leading model, like the NIST Cybersecurity Framework or ENISA's Interoperable EU Risk Management Framework, to align assessment and reporting across cognitive city systems.
- Establish dedicated task forces to monitor emerging technology trends and propose regulatory updates annually.
- Ensure comprehensive, clear, and detailed regulations delineate roles and responsibilities to foster effective collaboration and compliance.
- Develop clear governance structures that define specific roles and responsibilities for city officials, service providers, and citizens.
- Establish a regulatory sandbox program to evaluate innovative cybersecurity solutions in controlled environments before full-scale implementation.

Questions to Consider:

- What steps can our city take to continuously review and update our cybersecurity regulations to integrate emerging technologies such as AI and IoT?
- How can our city create a clear governance structure for cybersecurity that defines specific roles and responsibilities for city officials, service providers, and citizens? Could we use workshops and collaborative meetings to involve all stakeholders in the discussion and ensure clarity and buy-in?

3.2 Public-Private Partnerships (PPP)

Capitalizing on expertise and resources from both the public and private sectors is crucial for catalyzing the development of good cybersecurity solutions.

Integrating standardized procedures for incident response and enhanced information-sharing mechanisms is vital. Survey data supports this collaborative approach, with 30% of respondents identifying skill and expertise sharing as a critical component in public-private partnerships (PPP). The following points summarize our recommendations regarding PPP:

- Establish regular interface groups, including public and private sector leaders, to oversee joint cybersecurity initiatives.
- Develop standardized procedures for incident response and enhance information-sharing mechanisms across community stakeholders.
- Facilitate access to cutting-edge cybersecurity tools and solutions through public-private partnerships.
- Encourage collaborative efforts in developing novel solutions tailored to the unique needs of urban environments and the needs of their diverse residents.

Questions to Consider:

- How can we incentivize private sector participation in information-sharing initiatives while addressing liability and competitive advantage concerns?
- Which governance structures can ensure the equitable and efficient allocation of resources in joint public-private cybersecurity initiatives?

3.3 Skills and Talent Gap

Implementing effective training, recruitment, and retention programs is essential to cultivate a skilled cybersecurity workforce.

Ensuring personnel know the latest cybersecurity techniques and technologies is crucial, as 100% of respondents acknowledged a skills and talent gap. However, such investments must be considered as part of a long-term strategy.

Promoting continuous learning will empower the workforce and enhance the overall security posture of cognitive cities. Regarding 'direct' cybersecurity skills, such questions can be efficiently addressed through the use of a well-tested framework, such as that of the Swiss Cyber Institute (see Annex 1).

One should also pay proper attention to enhancing the 'indirect skills' that will benefit the advent of a secure urban environment. For example, experience shows that regulators with experience across sectors, cultures and avenues of life are generally more agile, innovative and impactful than those who come from a single training line (e.g., law, engineering or management). It is also crucial that city leaders and citizens have access to specific training and sensitization programs related to cybersecurity, data privacy, and digital transformation. The following points summarize our recommendations on the skills and talent gap:

- Establish a rotating fellowship program that allows cybersecurity professionals to gain experience across different sectors relevant to cognitive city operations, such as government, industry and academia.
- Promote continuous learning to update the workforce with the latest cybersecurity techniques and technologies.
- Consider the competitive nature of the job market and implement incentives and career development opportunities to retain skilled cybersecurity professionals.
- Focus on creating a conducive environment for career growth and professional development.

Questions to Consider:

- How can we redesign cybersecurity education to effectively integrate the multidisciplinary nature of cognitive city operations (e.g., IT, urban planning, public policy)?
- Which innovative incentive structures can be implemented to compete with often higher-paying private sector roles to attract and retain top cybersecurity talent in the public sector?

3.4 Data Privacy Protection Measures

Enforcing stringent access controls and deploying real-time monitoring systems are fundamental to safeguarding sensitive information.

Conducting regular security audits helps identify and rectify vulnerabilities, ensuring compliance with data protection regulations. According to 63.3% of survey participants, strict access controls and user authentication are paramount. The following points summarize our recommendations on privacy protection:

- Strengthen the enforcement of data privacy laws through more frequent audits and introducing new technologies to automate compliance checks.
- Ensure that all staff understand and uphold data privacy and ethics obligations.
- Leverage the latest security technologies, such as blockchain and advanced encryption, to enhance the security and integrity of data systems.
- Regularly update and audit security measures to identify and rectify vulnerabilities.

Questions to Consider:

- What practical steps can we take to strengthen the enforcement of data privacy laws in our city? Could this include more frequent audits or perhaps the introduction of new technology to automate compliance checks? How can we ensure that staff at all levels of the organization understand and uphold their obligations regarding data privacy and ethics?
- How can technical and policy measures be implemented to prevent the 'function creep' of data usage in cognitive city systems?

3.5 Human-Centricity

Human centricity refers to an approach that prioritizes people's needs, values, and well-being over technological or institutional considerations.

In contrast to 'technocentricity', human centricity is increasingly recognized as critical for advancing cities.[10] [11] Engaging residents in the cybersecurity policy-making process is essential to ensure that measures address real-world concerns and enhance the quality of life. Ensuring that cybersecurity solutions are accessible to all community segments fosters inclusivity and builds a comprehensive security posture. The following points summarize our recommendations regarding integrating resident feedback:

- Establish regular channels for residents to provide input on cybersecurity policies and practices, such as digital forums, town hall meetings, or dedicated surveys.
- Ensure that cybersecurity solutions address real-world concerns and enhance the quality of life for all residents.
- Develop initiatives to make cybersecurity measures accessible to all, including non-technical residents.
- Tailor communication and education efforts to diverse community needs, fostering inclusivity and building a comprehensive security posture.

Questions to Consider:

- How can we establish channels for residents to provide input on cybersecurity policies and practices? Could we consider digital forums, town hall meetings, or dedicated surveys?
- What steps can we take to ensure our cybersecurity initiatives are accessible to all, including non-technical residents, and sensitive to diverse needs?

To realize a human-centric vision for cybersecurity in cognitive cities, a comprehensive framework grounded in five guiding principles, **STEPS**, is proposed below:

Principle	DESCRIPTION
S – Solving Problems	Cybersecurity solutions should be driven by a genuine desire to solve residents' problems and address their concerns, rather than imposing top-down solutions. Citizen engagement and participatory processes are key to understanding and addressing the real needs of the community.
T – Transparency	Cybersecurity mechanisms must be transparent and understandable to citizens. Clear communication, educational initiatives, and open discourse are essential to build trust and alleviate fears surrounding privacy and security.
E – Exploratory	Cities should adopt an exploratory mindset, fostering a culture of testing, iterating, and involving citizen panels in the evaluation of potential cybersecurity solutions. This bottom-up approach ensures that adopted technologies align with the community's values and preferences.
P – Principle-Based	Cybersecurity and AI strategies must be designed and implemented in harmony with a city's overarching principles and objectives, such as sustainability, inclusivity, and accessibility. These technologies should enhance, rather than undermine, a city's core values.
S – Strategic	Cybersecurity should be embedded within a city's broader strategic vision and branding efforts. Showcasing expertise and know-how in this domain can position a city as a leader in the global smart and cognitive city landscape, attracting investment and talent.

Figure 11: Guiding principles for "STEPS" framework

4. Future Direction

In a VUCA (volatile, uncertain, complex, and ambiguous) world, cities are increasingly regarded as leaders in innovative solutions, often outpacing national responses to global challenges. Cities like Singapore and Lausanne exemplify the effectiveness of proactive strategies that anticipate future challenges and embrace innovative solutions.[12]

Their ability to adapt swiftly to new threats and to harness the benefits of technological advancements underscores their pivotal role in shaping future readiness. This is particularly evident in cybersecurity, where urban centers are integrating various emerging technologies — not just artificial intelligence (AI) but also the Internet of Things (IoT), big data, and blockchain. These technologies promise enhanced efficiency and improved civic engagement through applications like AI-driven traffic management systems and IoT-based public utilities monitoring. However, they also significantly expand the cybersecurity threat landscape.

Cities are witnessing a shifting landscape shaped by their developing use of AI and how both benign and malicious external actors deploy the technology. This dual-edged dynamic presents cities with unique challenges and opportunities.

Internally, cities are beginning to use AI to enhance service delivery, improve traffic management, and facilitate more responsive governance. These applications can streamline operations and make urban environments more livable and efficient.

However, adopting AI also means cities must safeguard these systems. AI systems can be exploited through various means, such as data poisoning, model theft, sophisticated phishing, and other social engineering or adversarial attacks, which could undermine the systems' integrity and functionality, leading to broader implications for public safety and trust.

Externally, cities must contend with the reality that actors outside their immediate control are also harnessing AI in ways that can impact urban life. This includes everything from multinational corporations and other states to non-state actors like hackers and private enterprises. These entities might use AI to align with or oppose a city's interests, such as competitive economic positioning, surveillance, misinformation campaigns, or direct cyber threats.

Cities must develop strategies that not only harness the benefits of AI for their communities but also protect and defend against its use by external forces.

This requires a robust cybersecurity framework that anticipates current threats and future challenges as AI technologies evolve. Cities need to invest in (and partner with) intelligence capabilities to continuously monitor and evaluate AI threats and trends, enhancing their defensive measures accordingly.

The collaboration between the public and private sectors plays a crucial role here. By leveraging partnerships with technology firms, cities gain access to state-of-the-art cybersecurity technologies and expertise. These alliances enable the creation of tailored cybersecurity solutions that protect against current and emerging threats. Furthermore, public awareness and community involvement are essential in fostering a culture of security. Educating citizens about the risks and benefits of new technologies enhances community resilience and trust in urban digital infrastructures.

The following points summarize our recommendations regarding improving the future readiness of cities:

- Implement proactive strategies that anticipate future cybersecurity threats and leverage technological advancements.
- Draw inspiration from cities like Singapore and Lausanne, which have demonstrated the effectiveness of proactive approaches in enhancing urban resilience.
- Develop robust cybersecurity frameworks by anticipating current and future challenges as AI technologies evolve.
- Collaborate with technology firms to create tailored cybersecurity solutions and continuously enhance defensive measures.
- Educate citizens about the risks and benefits of new technologies to foster community resilience and trust.

By implementing these comprehensive recommendations, stakeholders can significantly enhance the cybersecurity resilience and readiness of cognitive cities, ensuring that technology serves the people and improves their well-being and quality of life.

Annex 1

Target Skills Per Department

DEPARTMENT/ SECTOR	TARGET EMPLOYEE	TRAINING FOCUS	TRAINING FORMAT	LEARNING OBJECTIVES	LEARNING OUTCOMES
Government Administration and Regulatory Agencies	Policy Makers	Cyber Law and Policy	Interactive Webinars	Understand the legal framework governing cybersecurity	Ability to draft and interpret cyber policies
Defense and Intelligence Services	Intelligence Analysts	Advanced Cyber Threat Analysis	Classified Workshops	Analyze and counteract state-sponsored cyber threats	Mastery in intelligence-driven cyber defense strategies
Law Enforcement and Public Safety	Forensic Analysts	Cybercrime Forensics	Hands-on Labs	Investigate and solve cybercrimes	Expertise in digital evidence and crime scene investigation
Healthcare and Public Health	Healthcare IT Staff	Healthcare Data Protection	Scenario-based Training	Secure patient data and healthcare systems	Compliance with healthcare cybersecurity regulations
Financial Services and Revenue	Financial Analysts	Financial Cyber Risk Management	Online Training	Identify and mitigate cyber risks in financial operations	Implement financial data protection strategies
Energy and Utility Services	Operational Technology Staff	Critical Infrastructure Security	Field Exercises	Protect energy grids and utility services from cyberattacks	Ensure operational continuity under cyber threats
Transportation and Infrastructure	System Operators	Transportation Systems Cybersecurity	Simulation Exercises	Secure transportation networks and infrastructure	Resilience against cyberattacks on transportation systems
Education and Research Institution Policy Makers	Faculty	Academic Data Security	Interactive Lectures	Protect educational data and research integrity	Prevent academic data breaches and cyber theft
Information Technology and Telecommunications	Network Administrators	Network Security and Management	Hands-on Hacking Labs	Defend IT and telecommunications networks	Enhanced network security and incident response capabilities
Environmental and Agricultural Agencies	Environmental Scientists	Environmental Data Security	Online Training	Secure sensitive environmental data	Implement data integrity measures in environmental research
Municipal Services	City Planners, Municipal IT Staff	Smart City Cybersecurity	Virtual Workshops	Safeguard smart city infrastructures from cyber threats	Develop security protocols for urban technology systems
Judicial and Legal Services	Judges, Court IT Teams	Judicial System Cybersecurity	Online Training	Protect sensitive legal data and court systems	Ensure the integrity and confidentiality of judicial processes
Social Services	Social Workers, IT Staff	Data Protection in Social Services	Interactive Seminars	Secure personal and sensitive information of beneficiaries	Prevent unauthorized access to social service records and data
Cultural and Heritage Institutions	Museum Curators, Archivists	Cultural Heritage Cyber Protection	On-Site Training Sessions	Protect digital archives and cultural heritage from cyber threats	Implement security practices for digital and physical archives
Public Communication and Information Services	Public Relations Officers, Communication Teams	Secure Public Communications	Online Training	Ensure secure and trustworthy public communications	Mitigate risks of misinformation and protect against communication breaches
Energy and Utility Services (Renewable Energy)	Engineers and IT Staff	Renewable Energy Cybersecurity	Hands-on Workshops	Secure Energy Infrastructures	Implement security measures for renewable energy systems
Transportation and Infrastructure (Aviation)	Personnel in Airport and Flight Operations	Aviation Cybersecurity	Simulation Exercises	Protect aviation systems from cyber threats	Enhance cybersecurity measures in aviation systems

Annex 2

Survey Design and Key Steps

We designed our survey to capture insights from a diverse cross-section of industries, sectors and roles to ensure that our findings reflect the broad range of perspectives and experiences of stakeholders engaged in urban cybersecurity issues. We also ensured that emails and personally identifiable information (PII) were not collected to reduce the risk of a privacy breach.

Objective

The primary objective of this research is to gain comprehensive insights into the cybersecurity challenges and opportunities in cognitive cities. This study aims to identify vulnerabilities, assess current practices, and provide recommendations for enhancing cybersecurity in urban environments.

Survey Design

The research process and survey design were conducted in collaboration with multiple experts and institutions in the field of urban cybersecurity, representing the Knowledge Community of the Global Cybersecurity Forum Institute.

Data Collection

The surveys were distributed electronically and responses were collected securely and anonymously to ensure participant confidentiality. The data collection period spanned from April 2024 to May 2024. Survey distribution channels included professional networks, industry associations and media, and direct invitations to individuals with expertise in urban cybersecurity. An online survey platform was used to help with data collection.

Data Analysis

Data analysis encompassed both quantitative and qualitative approaches. Quantitative data was subjected to statistical techniques, which were employed to summarize responses to multiple-choice questions. Qualitative analysis involved thematic analysis of open-ended responses to identify recurring themes and insights.

Report Structure

The results of this research are organized into several main sections:

- **Vulnerability Landscape:** Analysis of the most vulnerable layers within cognitive city systems.
- **Collaborative Innovation and Governance:** Discussion on the importance of public-private partnerships, skill and expertise sharing, and the development of collaborative frameworks.
- **Data Privacy, Trust, and Ethics:** Examination of the key approaches to data privacy and integrity.
- **Navigating Regulatory Landscapes:** Insights into the adequacy of current regulations and areas for improvement.
- **Recommendations for Stakeholders:** Strategic recommendations for enhancing cybersecurity in cognitive cities.

Limitations and Ethical Considerations

The survey responses are subject to self-reporting bias, and the sample's representativeness depends on the participant's willingness to engage. Therefore, findings are based on the responses of participating city-focused leaders and may not be generalized to all cognitive city contexts. Ethical guidelines were followed to ensure the confidentiality and privacy of survey participants.

Acknowledgments

We want to thank the members of this Knowledge Community for their dedication and commitment to this initiative. Their expertise, participation and efforts have helped shape this global flagship report.

Special thanks go to the following individuals for their exceptional commitment:

- **Fahad Al Qahtani,** NEOM, Saudi Arabia
- **Hussain Aldawood,** NEOM, Saudi Arabia
- **Clay Garner,** SmartCitiesWorld, USA
- **Bruno Lanvin,** Smart City Observatory, Switzerland
- **Lee McKnight,** Syracuse University, USA
- **Chris Cooke,** SmartCitiesWorld, UK
- **Yusuf Abdul-Qadir,** Syracuse University, USA
- **Samir Aliyev,** Swiss Cyber Institute, Switzerland
- **Daniel González Bootello,** Smart City Cluster, Spain
- **Eduard Dumitrascu,** European Smart Cities Association, Romania
- **Hussain Alebnalshaikh,** University of Wollongong, Australia
- **Antonio Jara,** Libelium, Spain

We genuinely appreciate their contributions and look forward to continuing the collaborative efforts to secure the future of urban living. Thank you for your invaluable support and commitment.

Endnotes

1. Yin, Chuantao, Xiong, Zhang, et al. (2015). A Literature Survey on Smart Cities. Science China Information Sciences 58.

2. Bloomberg Philanthropies. (2023). Follow the Data Podcast: A New Frontier for Local Government: Generative AI. https://www.bloomberg.org/blog/follow-the-data-podcast-a-new-frontier-for-local-government-generative-ai/

3. Chowdhary, Rajat, and Hazem Galal. (2023). Cognitive Cities. https://www.pwc.com/m1/en/publications/documents/cognitive-cities-a-journey-to-intelligent-urbanism.pdf

4. Alahi, Md Eshrat E., Sukkuea, Arsanchai, et al. (2023). Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends.

5. Jara, Antonio J., Martinez, Iris, and Sanchez, Jaime. (2024). CyberSecurity Resilience Act (CRA) in Practice for IoT Devices: Getting Ready for the NIS2.

6. McKnight, Lee W., Smith, Danielle Taana. (2020). Smart Cities, Smart Bases and Secure Cloud Architecture for Resiliency by Design.

7. Kitchin, Rob. (2016). The Ethics of Smart Cities and Urban Science. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 374, no. 2083.

8. Serrano, Martin, Griffor, Edward, et al. (2022). Smart Cities and Communities: A Key Performance Indicators Framework.

9. Preis, Benjamin, and Susskind, Lawrence. (2022). Municipal Cybersecurity: More Work Needs to Be Done. Urban Affairs Review 58, no. 2: 614–29.

10. McBride, Keegan, Hammerschmid, Gerhard, and Cingolani, Luciana. (2022). Policy Brief: Human-Centric Smart Cities - Redefining the Smart City.

11. IMD / World Competitiveness Center .(2024). IMD Smart City Index 2024 Report. https://issuu.com/docs/e7a60c053affbf9e98fcba93afe857af.

12. IMD. (2024). By Striving to Be Globally Competitive, Cities Are Defining the Future. https://www.imd.org/ibyimd/future-readiness/by-striving-to-be-globally-competitive-cities-are-defining-the-future/


GLOBAL
CYBERSECURITY
FORUM
NEOM نيوم