



THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

GOVERNANCE OF TECHNOLOGY

Municipal data engines: Community
privacy and homeland security

NICK REESE

BALANCING
INNOVATION & CONTROL

a **wipro** company

#59 JUNE 2024

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

Editor

Shahin Shojai, Global Head, Capco Institute

Advisory Board

Lance Levy, Strategic Advisor

Owen Jelf, Partner, Capco

Suzanne Muir, Partner, Capco

David Oxenstierna, Partner, Capco

Editorial Board

Franklin Allen, Professor of Finance and Economics and Executive Director of the Brevan Howard Centre, Imperial College London and Professor Emeritus of Finance and Economics, the Wharton School, University of Pennsylvania

Philippe d'Arvisenet, Advisor and former Group Chief Economist, BNP Paribas

Rudi Bogni, former Chief Executive Officer, UBS Private Banking

Bruno Bonati, Former Chairman of the Non-Executive Board, Zuger Kantonalbank, and President, Landis & Gyr Foundation

Dan Breznitz, Munk Chair of Innovation Studies, University of Toronto

Urs Birchler, Professor Emeritus of Banking, University of Zurich

Elena Carletti, Professor of Finance and Dean for Research, Bocconi University, Non-Executive Director, UniCredit S.p.A.

Lara Cathcart, Associate Professor of Finance, Imperial College Business School

Géry Daeninck, former CEO, Robeco

Jean Dermine, Professor of Banking and Finance, INSEAD

Douglas W. Diamond, Merton H. Miller Distinguished Service Professor of Finance, University of Chicago

Elroy Dimson, Emeritus Professor of Finance, London Business School

Nicholas Economides, Professor of Economics, New York University

Michael Enthoven, Chairman, NL Financial Investments

José Luis Escrivá, President, The Independent Authority for Fiscal Responsibility (AIReF), Spain

George Feiger, Pro-Vice-Chancellor and Executive Dean, Aston Business School

Gregorio de Felice, Head of Research and Chief Economist, Intesa Sanpaolo

Maribel Fernandez, Professor of Computer Science, King's College London

Allen Ferrell, Greenfield Professor of Securities Law, Harvard Law School

Peter Gomber, Full Professor, Chair of e-Finance, Goethe University Frankfurt

Wilfried Hauck, Managing Director, Statera Financial Management GmbH

Pierre Hillion, The de Picciotto Professor of Alternative Investments, INSEAD

Andrei A. Kirilenko, Reader in Finance, Cambridge Judge Business School, University of Cambridge

Katja Langenbacher, Professor of Banking and Corporate Law, House of Finance, Goethe University Frankfurt

Mitchel Lenson, Former Group Chief Information Officer, Deutsche Bank

David T. Llewellyn, Professor Emeritus of Money and Banking, Loughborough University

Eva Lomnicka, Professor of Law, Dickson Poon School of Law, King's College London

Donald A. Marchand, Professor Emeritus of Strategy and Information Management, IMD

Colin Mayer, Peter Moores Professor of Management Studies, Oxford University

Francesca Medda, Professor of Applied Economics and Finance, and Director of UCL Institute of Finance & Technology, University College London

Pierpaolo Montana, Group Chief Risk Officer, Mediobanca

John Taysom, Visiting Professor of Computer Science, UCL

D. Sykes Wilford, W. Frank Hipp Distinguished Chair in Business, The Citadel

CONTENTS

GOVERNANCE OF TECHNOLOGY

08 Data and AI governance

Sarah Gadd, Chief Data Officer, Bank Julius Baer

20 “Data entrepreneurs of the world, unite!” How business leaders should react to the emergence of data cooperatives

José Parra-Moyano, Professor of Digital Strategy, IMD

26 Revolutionizing data governance for AI large language models

Xavier Labrecque St-Vincent, Associate Partner, Capco

Varenya Prasad, Principal Consultant, Capco

32 Municipal data engines: Community privacy and homeland security

Nick Reese, Cofounder and COO, Frontier Foundry Corporation

40 Human/AI augmentation: The need to develop a new people-centric function to fully benefit from AI

Maurizio Marcon, Strategy Lead, Analytics and AI Products, Group Data and Intelligence, UniCredit

50 Building FinTech and innovation ecosystems

Ross P. Buckley, Australian Research Council Laureate Fellow and Scientia Professor, Faculty of Law and Justice, UNSW Sydney

Douglas W. Arner, Kerry Holdings Professor in Law and Associate Director, HKU-Standard Chartered FinTech Academy, University of Hong Kong

Dirk A. Zetsche, ADA Chair in Financial Law, University of Luxembourg

Lucien J. van Romburg, Postdoctoral Research Fellow, UNSW Sydney

56 Use and misuse of interpretability in machine learning

Brian Clark, Rensselaer Polytechnic Institute

Majeed Simaan, Stevens Institute of Technology

Akhtar Siddique, Office of the Comptroller of the Currency

60 Implementing data governance: Insights and strategies from the higher education sector

Patrick Cernea, Director, Data Strategy and Governance, York University, Canada

Margaret Kierylo, Assistant Vice-President, Institutional Planning and Chief Data Officer, York University, Canada

70 AI, business, and international human rights

Mark Chinen, Professor, Seattle University School of Law

GOVERNANCE OF SUSTAINABILITY

82 Government incentives accelerating the shift to green energy

Ben Meng, Chairman, Asia Pacific, Franklin Templeton

Anne Simpson, Global Head of Sustainability, Franklin Templeton

92 Governance of sustainable finance

Adam William Chalmers, Senior Lecturer (Associate Professor) in Politics and International Relations, University of Edinburgh

Robyn Klingler-Vidra, Reader (Associate Professor) in Entrepreneurship and Sustainability, King's Business School

David Aikman, Professor of Finance and Director of the Qatar Centre for Global Banking and Finance, King's Business School

Karlygash Kuralbayeva, Senior Lecturer in Economics, School of Social Science and Public Policy, King's College London

Timothy Foreman, Research Scholar, International Institute for Applied Systems Analysis (IIASA)

102 The role of institutional investors in ESG: Diverging trends in U.S. and European corporate governance landscapes

Anne LaFarre, Associate Professor in Corporate Law and Corporate Governance, Tilburg Law School

112 How banks respond to climate transition risk

Brunella Bruno, Tenured Researcher, Finance Department and Baffi, Bocconi University

118 How financial sector leadership shapes sustainable finance as a transformative opportunity: The case of the Swiss Stewardship Code

Aurélia Fäh, Senior Sustainability Expert, Asset Management Association Switzerland (AMAS)

GOVERNANCE OF CORPORATES

126 Cycles in private equity markets

Michel Degosciu, CEO, LPX AG

Karl Schmedders, Professor of Finance, IMD

Maximilian Werner, Associate Director and Research Fellow, IMD

134 Higher capital requirements on banks: Are they worth it?

Josef Schroth, Research Advisor, Financial Stability Department, Bank of Canada

140 From pattern recognition to decision-making frameworks: Mental models as a game-changer for preventing fraud

Lamia Irfan, Applied Research Lead, Innovation Design Labs, Capco

148 Global financial order at a crossroads: Do CBDCs lead to Balkanization or harmonization?

Cheng-Yun (CY) Tsang, Associate Professor and Executive Group Member (Industry Partnership), Centre for Commercial Law and Regulatory Studies (CLARS), Monash University Faculty of Law (Monash Law)

Ping-Kuei Chen, Associate Professor, Department of Diplomacy, National Chengchi University

158 Artificial intelligence in financial services

Charles Kerrigan, Partner, CMS

Antonia Bain, Lawyer, CMS



DEAR READER,

In my new role as CEO of Capco, I am very pleased to welcome you to the latest edition of the Capco Journal, titled **Balancing Innovation and Control**.


The financial services and energy sectors are poised for another transformative year. At Capco, we recognize that this is a new era where innovation, expertise, adaptability, and speed of execution will be valued as never before.

Success will be determined based on exceptional strategic thinking, and the ability to leverage innovative new technology, including GenAI, while balancing a laser focus on risk and resilience. Leaders across the financial services and energy industries recognize the transformative benefits of strong governance while needing to find the optimal balance between innovation and control.

This edition of the Capco Journal thus examines the critical role of balancing innovation and control in technology, with a particular focus on data, AI, and sustainability, with wider corporate governance considerations. As always, our authors include leading academics, senior financial services executives, and Capco's own subject matter experts.

I hope that you will find the articles in this edition truly thought provoking, and that our contributors' insights prove valuable, as you consider your institution's future approach to managing innovation in a controlled environment.

My thanks and appreciation to our contributors and our readers.



Annie Rowland, **Capco CEO**

MUNICIPAL DATA ENGINES: COMMUNITY PRIVACY AND HOMELAND SECURITY

NICK REESE | Cofounder and COO, Frontier Foundry Corporation¹

ABSTRACT

Convergence is when two or more separate technologies are paired together to create a capability that is greater than the original technologies individually. The additional value of the converged system itself now opens new applications as well potentially new challenges. As policy conversations around emerging technology implications grow, the importance of considering convergence is paramount for effective and trustworthy implementation of technologies in municipal spaces. A connected community is not a technology but a convergence concept that touches millions of citizens, their privacy, and the critical infrastructure on which each of them depend. As with all examples of convergence, there are implications beyond the sum of their parts and connected communities is no exception. Officials and individual users are familiar with the implications of connected technologies on individual privacy but the concept of municipal, community, or regional privacy is new. The aggregated data of an entire community or region take the concept of privacy to the homeland security level, driving increased need for effective policies and controls to ensure the safety and security of citizens living inside these architectures. This article explores specific challenges for the implementation of municipal IoT and introduces the concept of privacy at the municipal, community, and regional levels.

1. INTRODUCTION

Emerging quickly and seemingly without warning, generative artificial intelligence (GenAI) reignited series of debates around governance, ethics, and technology proliferations and its impact on any number of aspects of the human condition from romantic relationships to human job loss to national security. For governments and policymakers, the topic of AI had been an area of general interest and discussion, but the introduction of ChatGPT in November of 2022 has accelerated debate and action. In the U.S, a new AI Executive Order was released by the Biden Administration [White House (2023)] and the European Union (E.U.) passed its AI Act [European Parliament (2023)]. While much of the debate around AI has thus far focused on specific models, ownership, output quality, security, or ethics, the issue of technology convergence has been largely absent from the discussion.

Convergence is when two or more separate technologies are paired together to create a capability that is greater than the original technologies individually. The additional value of the converged system itself now opens up new applications as well potentially new challenges. For example, unmanned aerial vehicles (UAV) or drones combine technologies that include computer optics, robotics, AI, telecommunications, aerospace technologies, and more. Alone, each of these technologies is significant but when paired together and aimed at a specific use, they form something completely new that is greater than any of the individual technologies that make it up. In the same way, convergence of other technologies is creating bigger challenges than the mere existence of GenAI tools. Convergence between cutting edge technologies like AI and quantum or outer space capabilities and AI have the potential to create far bigger impacts and should be addressed.

¹ The author holds a faculty position at New York University, where he teaches courses on Emerging Technology and National Security and on Connected Communities. He is a member of the Homeland Security Advisory Board at George Washington University and is the former Director of Emerging Technology Policy at the U.S. Department of Homeland Security.

A trap when talking about technology concepts is to keep them overly abstract. Talking about AI as a general concept leads to abstraction that borders on uselessness. The same can be true when talking about convergence. It is a generally easy concept but without a real use case, it can feel like much less of a factor than it is. Rather than discuss convergence as a concept, this article will use the application of convergence in municipal environments as a way to properly convey the message and the challenges.

Known as “smart cities” or “connected communities”, connected technology deployments in municipal environments, rural and urban, is growing. Citizen demand for such technologies is also growing as potential solutions for traffic problems, energy use, and resource distribution, among others, are proposed. There are few technology architectures that impact more people more directly than a connected community deployment in a municipal environment of any size. Internet connected devices that monitor and optimize our resource distribution also create cyber vulnerabilities where none previously existed. The study of critical infrastructure risk and dependence has been ongoing for years but the addition of potentially tens of thousands of connected devices to critical infrastructure without a standard method of deployment or security requirements renders most of the cyber risk assessments void. Technology convergence is becoming a serious potential threat to our homeland security and our ability to provide critical services, and it impacts more people directly, and through their data privacy concerns, than any technology individually.

In this article, we will explore what a connected community is, what technology comprises its architecture, and discuss the gaps we see as these architectures continue to be developed and deployed on top of critical infrastructure. We will explore privacy issues, not at the individual level but at the municipal level, and show how municipal privacy extends to a homeland security issue rather than a law enforcement issue. Finally, we will discuss the need for new risk models, powered by AI, and for interoperability of connected community technologies. Technology convergence is an issue that will touch everyone, but no single use case will touch as many as connected communities.

2. WHAT IS A CONNECTED COMMUNITY

In a 2020 literature review, multiple authors define the term “smart cities” as generally referring to the use of technology-based solutions to enhance the quality of life for citizens, improve interactions with government, and promote sustainable development [Ismagilova et al. (2020)]. A smart city, or connected community, is not itself a technology, rather it is a concept and a perfect example of convergence. A connected community seeks to bring deployed technologies to bear against problems in municipal environments. The specific problems that are targeted for solution depend heavily on the municipality itself. For example, a rural community may choose to incorporate a smart irrigation system into its architecture while urban environments may choose to focus on traffic issues or WiFi in public spaces. On some levels, a connected community architecture must function this way because the implementation of technology in a municipal environment must directly reflect the needs and realities of the municipality in question. What works for Pittsburgh may not work for Seattle because of the different needs and environments of each city. In all cases, architectures bring some combination of the following technologies to form a foundation that seeks to solve a given set of municipal problems:

- internet of things (IoT) (sensors/devices)
- telecommunications (5G, nG)
- cloud
- artificial intelligence (AI)
- mobile applications
- WiFi-7
- Industry 5.0 [Javed et al. (2022)].

This foundation creates specific capabilities such as smart traffic monitoring, smart energy distribution, smart sewer systems, and many more. One, some, or all of these capabilities may be woven together to create the specific architecture for the given municipality. A connected community is not one thing; instead, it consists of a customized architecture of different emerging technology applications that are specific to the needs of the municipality. How the architecture is configured can have a significant impact on the citizens of the municipality (urban or rural), in addition to the critical infrastructure upon which the technologies are deployed.

3. DATA GENERATORS AND AGGREGATORS

With so many ways to think about a connected community, the best way is to think of it as a giant data generator and aggregator. In a 2021 study of published literature on smart cities, Ullah et. al. (2021) studied the top technological and organizational risks to connected community architectures based on appearances in peer reviewed articles. According to that study, the top two technological risks were IoT and big data integration, while the top two organizational risks were user data security and data safety. A given architecture might consist of tens of thousands of connected IoT devices. Those devices collect information constantly, possibly close to real time. All those devices are connected via a 5G, or ubiquitous WiFi connection, and they report their results likely to a cloud. In the cloud, some form of data analytics is performed, likely by AI.

The results of that analysis must be shown to human operators in some form, whether as near-real time data flow or as an analysis report. From there, some adjustment is made to the urban environment either automatically or by data-informed humans. As an example, placing connected IoT devices on the homes of people in a municipality to monitor their electrical use can have huge benefits for the grid and for the power generation plant serving the community. In this case, the IoT devices would be collecting real time electricity use data and transmitting it back for analysis. After the analysis is complete, municipal leaders may choose to change the electrical plant's output to mirror the demand more closely.

Whether we are talking about an electrical plant, sewer monitor, or traffic system, deploying tens of thousands of internet-connected devices in the municipal environment will result in enormous volumes of data being generated and aggregated. The economic and geopolitical value of data is hardly in doubt nor its ability to adversely impact individuals if not properly protected. A reality of connected community architectures, regardless of how they are configured, is that they will generate and aggregate huge volumes of data on both individuals and entire municipalities, potentially entire regions.

Bibri (2019) discusses the emergence of big data in the municipal environment, but from the perspective of contributions to sustainability and sustainable urban practices. The study does not, however, highlight the potential for exploitation of architectures by malicious actors nor the homeland security impacts of data aggregation at the municipal level. While it does discuss the need for public

privacy and security, this literature review was focused on the components functioning together as intended revealing a gap in security standards discussions in the connected community arena.

The U.S. government provided a specific standard in September 2020 for the "Security and privacy controls for information systems and organizations" in the National Institute of Standards and Technology (NIST) special publication 800-53 [NIST (2020)]. The document provides "a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks." While 800-53 provides important practices and guidelines, it is necessarily high level and lacks the specificity demanded by a convergent system of different devices. Second, the standard, while used widely, is not compulsory, leaving connected community architectures in an uncertain state depending upon whether municipal leaders decide to demand adherence to the standard by policy or contract language. A system that displays the level of convergence seen in connected community architectures demands a more specific standard for both cybersecurity and privacy controls at the technical level and should be paired directly with municipal or state policy and assigned an accountable official.

4. PRIVACY AND INTEGRATED RISK AT THE MUNICIPAL LEVEL

Most discussions on the topic of online privacy surround an individual's right to security of data and agency of their personal data. This conversation is indeed important and the imperative to protect the data and maintain the privacy rights of individual users online is critical and should continue to be the subject of efforts to improve. The nature of connected community architectures is that they collect and aggregate the personal data from thousands or millions of individuals. Viewed through the lens of personal privacy, this issue requires significant attention as it presents an attractive target for would-be malicious cyber actors. The potential for criminal cyber activity, as well as state-sponsored, geopolitically motivated cyber actions, is extremely high and individuals should have some level of assurance on how their data is being collected, stored, and used. When viewed through the lens of the entire municipality, the collection of these data takes on a different characteristic.

The theft of the personally identifiable information (PII) of an individual or group of individuals through a cyberattack is a serious issue that deserves the resources of the proper authorities, and the best efforts of cybersecurity professionals, to prevent. Stepping back from the view of privacy as an individual issue, the larger, and perhaps more impactful issue, is around the privacy of the municipality. The exposure or theft of PII of an individual, with its public apologies and promises of free credit monitoring, is serious for the individual, but in nearly all cases would not rise to the level of a homeland or national security issue. In the case of a municipality of any size, the pooled data about the behaviors and working of that municipality, as collected by connected community architectures, represents a potentially frightening new aspect of privacy – the privacy of an entire municipality.

Spicer et. al. (2023) found a “sharp divergence between the smart city services being put in place by municipal administrators and the types of services residents want to see.” This finding raises questions about how aware citizens are about the individual data and privacy issues and the broader municipal scope of the issue. Architectures that are implemented should not only address direct issues with municipal functions but also include public education and communications plans to create an informed resident population.

Architectures provide data that help leaders analyze municipal functions and adjust to optimize for a given goal. For example, the reduction of traffic in certain areas at certain times or the distribution of electrical energy at peak and off-peak times. That same information provides insights that can just as easily be used for malicious purposes. In the transportation example, a municipal planner might use deployed IoT devices to measure what subway stations are the most crowded at what times to determine how many cars should be running at peak hours. That same data could be used by a malicious actor to determine the best area to place an explosive device for maximum impact. Similarly, efficient electrical energy distribution is key to ensuring equitable critical infrastructure services in growing urban environments. The same information could be used by a malicious cyber actor to determine the best grid(s) to disrupt with a cyberattack against the energy system.

Both examples above unambiguously represent homeland security threats that are far beyond the scope of the normal privacy policies and measures. An underappreciated and understudied aspect of installing a connected community architecture in any municipality is the potential for the collected and aggregated municipal data to become a significant homeland or national security threat. Privacy policies regarding connected communities should not focus only on individual privacy but on the privacy of the municipality. At the national level, the Department of Homeland Security (DHS), through the Cybersecurity and Infrastructure Security Agency (CISA), should study the risks to entire critical infrastructure sectors related to the number of connected community architectures in each region. A large city like New York, Chicago, or Los Angeles would clearly have potentially hundreds of thousands or millions of deployed IoT devices in their municipalities, making the risk more obvious than if a collection of small- or medium-sized municipalities had small architectures. Depending on where each was located and how they were configured, the risk to critical infrastructure from a theft of connected community data could be equivalent in either case.

The security of pooled data at the municipal level represents a potential homeland or national security issue if a malicious actor accessed the data and decided to use it as a whole, rather than to steal the PII of an individual or group of individuals. Policies and cybersecurity measures should be designed to account for the privacy of the entire municipality, leading to cyber incident response procedures that mitigate possible attacks against the broader community or region. The introduction of deployed IoT devices into our municipalities may be proven to be a necessity as we cope with growing urban populations, the need for higher agricultural yields, more efficient energy distribution, and more. However, by definition, these devices are connected or adjacent to critical infrastructure systems that were heretofore not connected to the internet. The introduction of tens or hundreds of thousands of potential access points where there used to be zero is a significant change in the risk profile for any critical service and it is made more important by the fact that these systems are serving some of our largest population centers. That makes for both a fertile ground for criminal theft of individual data and of potentially more dangerous theft of the municipality’s data. With the target this enticing and the impact this great, the first step towards more security in connected communities is through the creation of interoperability standards.

5. INTEROPERABILITY AND RESILIENCE

In October of 2022, a little-known industry group published a technical standard that most have likely never heard of. It was called Matter² and it was developed by the Connectivity Standards Alliance.³ What they created was a protocol standard that allows smart home IoT devices to work together regardless of brand. You may have a smart speaker built by Apple in your home and with Matter you can buy smart devices from Google and other companies and integrate them into your home network natively. The importance of interoperability can be overlooked but it is a critical element of cybersecurity, and it is particularly important for connected communities. Javed et al. (2022) found that interoperability was listed as the top requirement for future smart cities. The first major gap in the deployment of connected community architectures is in interoperability standards and there is a template for how to do it.

A search for connected community components will yield no shortage of companies that are happy to provide their solution to your municipality. As an example, one company (name omitted) will provide you with a package that includes:

1. IoT sensors in a variety of functions.
2. Private 5G network for connectivity.
3. Cloud infrastructure for data storage.
4. AI for data analytics.
5. A slick dashboard for monitoring all devices.

That is an end-to-end, turnkey solution that is attractive to municipal leaders who do not want to waste time and go through contracting processes more than once. The problem, easily visible to any cybersecurity professional worth their salt, is that this network is not resilient. A single vulnerability could potentially take the entire network down, since this is an end-to-end solution. Interoperability does not eliminate cyber vulnerabilities, but it does increase the potential that an attack will be stopped at one component in the chain. If all components are built by a single company, they are likely to have common vulnerabilities among them. If the architecture

includes components from a variety of vendors, it is less likely that a single vulnerability will bring down the entire system. This is called vendor diversity, and it is an excellent way to build resilience into any network of devices.

This was part of the reason behind the development of the Matter standard, as the alliance recognized the resilience inherent in this solution. If it was recognized for individual homes, how has it been overlooked for municipal environments? The imperative to create a protocol standard for interoperability is analogous to the discussion on individual privacy versus the privacy of a municipality. While it is certainly important to increase vendor diversity in home IoT, vendor diversity is extremely important for municipal IoT given its proximity to critical infrastructure. As more municipalities roll out plans for connected community architectures, they need to have the option to include interoperable equipment as a cybersecurity and resilience measure.

6. DEPLOYMENT STANDARDS

The next gap in deployments is the lack of minimum requirements for architecture deployments. Part of the attraction of the connected community concept is that it is not a one-size-fits-all solution that may or may not work for a given municipality. Communities can, in theory, choose for themselves which challenges they can solve using technology deployments and how to best roll them out for the community's needs. That flexibility should remain a feature of connected community deployments, but it is too important to leave entirely to the discretion of community officials. Connected community architectures have the potential to directly impact critical infrastructure, large numbers of citizens, and to devolve into actual homeland or national security issues. These realities demand the creation of minimum cybersecurity standards that apply to municipal environments. The National Institute for Standards and Technology (NIST) is well equipped to create such a standard through its Global Community Technology Challenge.⁴ With the help of CISA's Infrastructure Security Division,⁵ the federal government could create the minimum standard required to ensure a cybersecurity baseline for all connected community deployments.

² <http://tinyurl.com/23vhwcr>

³ <http://tinyurl.com/4km4zuat>

⁴ <http://tinyurl.com/yycr2n66>

⁵ <http://tinyurl.com/mks6269m>

7. POLICY GAPS

The final gap is in the policy apparatus of municipalities. It is critically important that connected community architectures be chosen according to defined municipal challenges and aligned with a strategic vision. Municipalities should have accountable officials in place to oversee not only the deployment but the long-term operation of the system. Small issues like missing a firmware update on a single deployed sensor could result in an attack vector that causes extreme damage, and someone must be accountable to ensure the integrity of the system. The following recommendations are provided to help community leaders build the required foundation for successful connected community deployments.

1. **Unifying strategy:** a 2023 study of twelve cities in Spain with a total of 1,625 smart initiatives found that formal strategic planning was the main tool used in successful implementation of smart initiatives [Bolívar et al. (2023)]. Strategic guidance provides the vision for a connected community project and provides answers to questions about why certain decisions were made. A unifying strategy should give municipal officials, at any level and in any department, a piece of paper to which they can point to justify the actions they are taking. The strategy should be public in an effort to maximize transparency. Examples of issues that should be covered:

- overarching priorities
- specific problems to be solved
- potential challenges
- statement on risk identification and mitigation
- public outreach plan.

2. **Accountability trinity:** accountability is the key to ensuring that policies are carried out into action. In the municipal environment, there are three offices that must be filled with an individual who is individually accountable and not wearing multiple hats. Given the amount of data being generated, the privacy implications, and the potential for security risks, the following positions are critical for creating an accountability trinity that will ensure the operationalization of priorities from the “unifying strategy”:

- Chief Information Officer
- Chief Privacy Officer
- Chief Information Security Officer.

3. **Map of deployed devices:** one of the biggest threats to connected community architectures is a cyber vulnerability in a single, seemingly unimportant, deployed sensor. If that sensor does not receive, or successfully install, a critical firmware update or patch, the entire architecture is in jeopardy and the risk to critical infrastructure services increases. To ensure the integrity of the entire system, a live map of the real time status of deployed sensors will provide human operators with the ability to see potential issues and respond to them quickly. In the absence of such a capability, a single sensor could provide the access point required by malicious cyber actors, which is the first step in a downstream attack that could escalate to create effects exponentially more damaging than accessing a single sensor.

4. **Contracting language:** one of the most powerful tools municipal leaders have is their contracting language. If contracts stipulate that the vendor adhere to a set of standards aligned with the unifying strategy, vendors will have to adjust if they want the contract. Municipal leaders should deep dive into procurement processes and contracting language and find ways to ensure the security measures they prioritized in their strategy. This also gives the public the peace of mind to know that the strategy is not just words.

5. **Public communications plan:** transparency is foundational to any connected community plan and should include a robust public communications plan. At minimum, this plan should consist of the following elements:

- **Early outreach:** in this phase, municipal leaders should engage the public on the challenges they see and how they believe technology can solve them.
- **Priorities:** the priorities, through the unifying strategy, should be public and promoted, not buried on a municipal website.
- **Crisis communications:** in the event of a cyber event, the municipality should be prepared to communicate with the public and provide updates on the state of the crisis.
- **Public education:** the municipality should build in outreach that provide education about what purposes technologies will serve and how they will benefit the community. These programs should include technical literacy courses, upskilling, basic cyber hygiene, and privacy rights.

8. CONCLUSION

Connected community architectures are already being deployed in the U.S. and around the world, and for good reasons. Growing urban populations and the need to make resource distribution more efficient and equitable are driving the implementation of technological solutions. The rollout of 5G was a major driver of the technological convergence in the municipal environment, providing the bandwidth to support thousands more deployed IoT devices. It is possible that large urban environments of the future will require connected community architectures to function, so it is critical that these deployments be executed in a way that inspires public trust and prioritizes security and resilience. Deployed IoT devices that monitor critical elements of municipal functions are able to gain impressive insights that help planners and officials create better communities. There are also some risks that have to be recognized, planned for, and mitigated to the best of our collective abilities. Below are a few important factors that need to be taken into consideration when considering a connected community deployment:

- **Can the identified problem be solved by a technology solution?** There have been suggestions that deployed IoT and the right AI algorithms can cure all municipal ills from traffic problems to social inequality. The reality is that the scope of what deployed IoT devices can solve is limited. These solutions, as they exist today, are best at finding efficiencies and optimizing services such as electricity, traffic, or water/sewage services. They are also very good at increasing access to information such as through public WiFi programs or municipal mobile applications that allow for better access to services. However, there is a limit and a connected community architecture, no matter how well designed, will not solve every problem. It is imperative that municipal leaders spend time on what the problem actually is, what its secondary impacts are, and whether it is feasible for a technological deployment to solve it.
- **Does the municipality have the internal resources to manage the architecture long-term?** As with any technology project, there is a lifespan and maintenance tail that has to be accounted for by municipal leadership. Even if there are specific provisions in the contract for the company to provide services, the municipality still must have people who can monitor and evaluate the

performance of the system and ensure its integrity. A community without the accountability trinity, or without sufficient staff to stay engaged with the architecture over its lifespan, is destined for trouble. Part of the evaluation on whether to support and implement a project should be a self-evaluation that looks at the community's capacity to operate the system in the absence of vendor support.

- **In what ways is public engagement built into the deployment?** This is a multi-phased issue that must start at conception and run through upkeep and potential crises. Key to this is education of the public on technology literacy and basic cyber hygiene. Implementation of architectures without public outreach and education will also encounter problems throughout the life of the system in the form of potential trust issues.

Connected community architectures are already in effect in multiple U.S. and global cities, but they lack a basic level of standardization that would allow security and resilience measures to be implemented to protect vulnerabilities to critical infrastructure. These localized systems, even if implemented in small municipalities, could become the critical cyber vulnerability that introduces risk to national critical functions and critical infrastructure sectors. That kind of systemic risk ultimately trickles down to specific systems and individual components but can escalate throughout the national structure. Direct cyber vulnerabilities to critical infrastructure are reason enough to enforce minimum standards, but the potential for a breach of municipal or regional data could result in even more catastrophic events. Between these two vulnerabilities, basic interoperability standards should be created and implemented, and basic security standards should also be enforced. This is not a call for regulation but for a recognition that the technology convergence that is providing us with the insights to optimize our municipalities also carries the potential to catastrophically disrupt it. Connected community technology is exciting and may prove critical to resource distribution and services in the coming years as urban populations grow. The interest in these architectures as a cyber target will also grow and it is incumbent on cyber professionals and policymakers to start mitigating risks now.

REFERENCES

- Bibri, S. E., 2019, "On the sustainability of smart and smarter cities in the era of big data; an interdisciplinary and transdisciplinary literature review," *Journal of Big Data*; Article 6:25, <http://tinyurl.com/tu2bkdp>
- Bolivar, M. P. R., L. A. Munoz, and C. A. Munoz, 2023, "Identifying patterns in smart initiatives' planning in smart cities. An empirical analysis in Spanish smart cities," *Technological Forecasting and Social Change* 196, <http://tinyurl.com/4bkpump>
- European Parliament, 2023, "European Union Artificial Intelligence Act," December 19, <http://tinyurl.com/3449ysr3>
- Ismagilova, E., L. Hughes, N. P. Rana, and Y. K. Dwivedi, 2020, "Security, privacy, and risks within smart cities: literature review and development of a smart city interaction framework," *Information Systems Frontiers* 24, 393-414
- Javed, A. R., F. Shahzad, S. ur Rehman, Y. Bin Zikria, I. Razzak, Z. Jalil, and G. Xu, 2022, "Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects," *Cities* 129, <http://tinyurl.com/4nvc7uc>
- NIST, 2020, "Security and privacy controls for information systems and organizations," Department of Commerce, NIST SP 800-53, Revision 5; September, <http://tinyurl.com/2s4vpa5n>
- Spicer, Z., N. Goodman, and D. A. Wolfe, 2023, "How 'smart' are smart cities? Resident attitudes towards smart city design," *Cities*, Volume 141, <http://tinyurl.com/ydkfxbbf>
- Ullah, F., S. Qayyum, M. J. Thaheem, F. al-Turjman, and S. M. E. Sepasgozar, 2021, "Risk management in sustainable smart cities governance: a TOE framework," *Technological Forecasting and Social Change* 167, <http://tinyurl.com/25k72bk3>
- White House, 2023, "Executive Order on the safe, secure, and trustworthy development and use of artificial intelligence," Biden Administration, October 30, <http://tinyurl.com/2rbvbnap>

© 2024 The Capital Markets Company (UK) Limited. All rights reserved.

This document was produced for information purposes only and is for the exclusive use of the recipient.

This publication has been prepared for general guidance purposes, and is indicative and subject to change. It does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (whether express or implied) is given as to the accuracy or completeness of the information contained in this publication and The Capital Markets Company BVBA and its affiliated companies globally (collectively "Capco") does not, to the extent permissible by law, assume any liability or duty of care for any consequences of the acts or omissions of those relying on information contained in this publication, or for any decision taken based upon it.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC

Bengaluru – Electronic City
Bengaluru – Sarjapur Road
Bangkok
Chennai
Gurugram
Hong Kong
Hyderabad
Kuala Lumpur
Mumbai
Pune
Singapore

MIDDLE EAST

Dubai

EUROPE

Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
Glasgow
London
Milan
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA

Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto

SOUTH AMERICA

São Paulo

WWW.CAPCO.COM



CAPCO
a wipro company