Risk, resilience and security for governments and cities

Best practices and technologies to maintain business continuity

Alcatel·Lucent Enterprise

Table of contents

Security and resilience are urgent priorities

Today, governments and cities around the globe are facing a polycrisis, that is, a convergence of cyber and physical risks that threatens citizens, critical services and sensitive data.

Citizens now expect, and rely on, services provided through secure websites, and employees expect to work from home or in the office, based on their needs and preferences. These new requirements, along with the exponential spread of Internet of Things (IoT) devices, extend network boundaries at a time when geopolitical tensions and political polarisation are increasing the risk of cyberattacks.

Additionally, the dark web has created a profitable marketplace to anonymously sell sensitive government data, making government systems very attractive targets for information theft. It also provides an online haven to coordinate attacks on governments.

Vandalism, terrorism, riots and crime are also on the rise, creating ever-greater threats to civic and defence infrastructure and business continuity. Add to that, severe weather events and natural disasters that make it very difficult, if not impossible, to deliver government services and keep citizens safe when they need it most. And, with global inflation straining budgets, the need for digitalisation initiatives that increase operational agility, efficiency and productivity has never been greater.

Together, these risks are making it more difficult than ever for governments and cities to remain fully compliant with increasingly strict data sovereignty and privacy regulations. As a result, there's considerable potential for infringement fines and lawsuits.

Faced with this new reality, governments and cities can no longer rely on their previous strategies for security and resilience. To mitigate these risks, they must take bold, proactive steps to improve their overall security posture. A fresh and innovative approach that's more closely aligned with today's most significant threats is required. With enhanced security, governments and cities will be better positioned to protect citizens and operations and strengthen their resilience so they can ensure business continuity in any circumstances.

The risks are real

Unfortunately, it's all-too-easy for governments and cities to delay risk mitigation measures, especially when newsworthy incidents are only occurring in far-away locations. But the reality is, every government organisation is a potential target for attacks.

A reality check

- Cyberattacks against governments jumped 95 percent in the last half of 2022.[1]
- The attack on the government of Costa Rica was considered to be one of the costliest attacks of the year,[2] with ransomware a favoured method of attacks on public services.[3]
- By 2025, it's estimated that 30 percent of critical infrastructure organisations will experience a security breach.[4]

As city populations continue to grow,[5] the risks for governments and citizens increase. The United Nations is advising governments to work to make cities and human settlements more inclusive, safe, resilient and sustainable, as published in Goal 11.[6]

---

[1] Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says. CSO United States, January 2023.

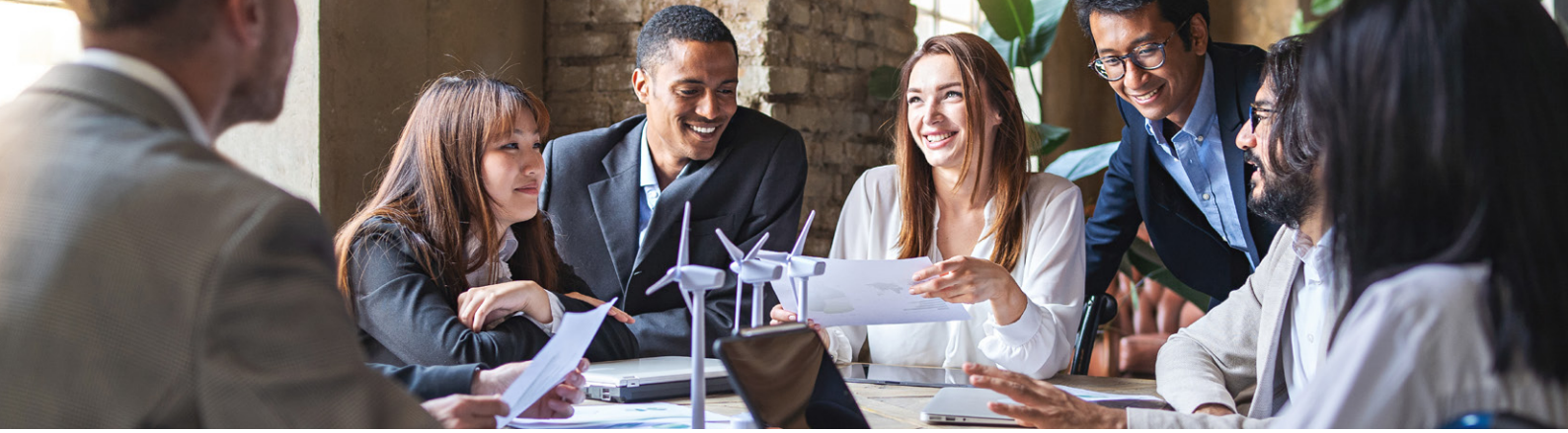
[2] The 13 Costliest Cyberattacks of 2022: Looking Back. Security Intelligence, December 2022.

[3] Policy paper: National Cyber Strategy 2022. U.K Cabinet Office, December 2022.

[4] Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025. Gartner, December 2021.

[5] Urban Development. The World Bank, April 2023.

[6] Goal 11: Make cities and human settlements inclusive, safe, resilient and sustainable. United Nations.



With all of these factors in mind, it's clear that governments and cities must put renewed focus on risk, resilience and security to:

- **Ensure continuity of critical services and protect sensitive data**, particularly in times of unexpected crisis
- **Minimise risk insurance costs** by implementing the right protection for each type of cyber and physical risk they face
- **Reduce financial losses** due to cyber and physical attacks, prosecution by citizens, and fines for data breaches and non-compliance
- **Maintain their reputation and citizens' trust**, both of which can be damaged or lost completely due to service delays and outages
- **Safeguard citizens** by providing important information related to health, safety and protection

Digitalisation brings benefits and risks

In today's digital world, people, objects and processes are connected. These connections empower governments and cities to:

- Take advantage of IoT technology and the information it provides
- Automate workflows to increase efficiency and accelerate responses to citizens
- Use accurate, real-time data to increase visibility and make informed decisions
- Implement smart building applications that enable more sustainable, cost-effective and resilient operations

While these improvements are essential for governments and cities to achieve their goals, the enabling technologies also introduce a new set of cyber and physical risks that must be addressed.

New ways of thinking about vulnerabilities

With digitalisation, vulnerabilities are easier to expose, and threats can quickly cascade throughout interconnected systems, devices and applications:

- A failure in one system can affect all
- Hackers can exploit connections between infrastructures to extend their reach
- Viruses can take advantage of the connections to propagate throughout an organisation

Digitalisation also tightens the connection between cyber and physical risks. For example, bad actors can remotely hack into government data centres or gain physical access by compromising an electronic door lock. Similarly, security cameras can be disabled, disconnected, or reconnected to pre-recorded video feeds through a cyber or physical attack, making them useless from a protection perspective in either case.

Convergence between IT and operational technologies (OT) creates new opportunities for attacks. Now, hackers can compromise an IoT sensor to gain access to the network and the high value systems and information resources connected to it. Conversely, they can hack into the network directly, using it as a gateway to attack critical building systems such as elevators, smoke detectors, fire alarms and sprinkler systems.

New technologies can also be used for and against government organisations. Take artificial intelligence (AI) as an example. AI helps to prevent, protect against and accelerate responses to cyber and physical threats, but it also empowers bad actors to crack passwords to government systems. In the future, we can expect a similar situation with quantum computing, which will help governments solve complex problems but also make it easier to decrypt sensitive information.

Unique considerations and challenges

The specific risks introduced with digitalisation depend on the technologies being deployed. Modern networks and communications technologies bring three main risks:

- **Breakdowns**: Hardware and software faults and failures can occur at any time, without warning. Fires, floods, extreme weather and other unforeseen factors can also cause breakdowns, while power failures can affect the quality and stability of power delivery, leading to malfunctions and failures.
- **Cyberattacks**: Confidential data can be lost or stolen, and networks and systems can be corrupted, slowing or stopping government services and operations altogether. Ransomware attacks can hold entire networks and systems hostage, making data and critical functionality inaccessible.
- **Obsolescence**: Technology providers can end support for hardware and software, while supply chain shortages can make it logistically impossible or too expensive to continue using solutions. Changes to regulatory compliance requirements can also render technology solutions obsolete.

Each of these risks can lead to the others. A breakdown or obsolete technology can open the door to cyberattacks. And cyberattacks can cause a breakdown or highlight that technology is now obsolete.

Together, these risks mean governments and cities must improve their ability to prevent, protect against and react to threats. Doing nothing is no longer an option. Continuing to rely on outdated and isolated networks and communications technologies as risks continue to multiply is not a viable approach from any perspective.

A holistic approach and standardised process

Each government and city must develop a strategic and tactical approach to security and resilience that's tailored for their unique risk profile, geographic location, mandate, budget and other requirements. However, while the results of their efforts will differ, there is value in taking a standardised approach and sharing best practices for better outcomes.

A holistic approach to risk mitigation allows governments and cities to increase security and resilience across three key areas of their mandate which include:

- **Citizens**: To protect human safety and data from all threats
- **Operation**s: To maintain secure and reliable functions, transactions and services in all circumstances
- **Buildings**: To make government workplaces and spaces smarter and more secure

Four steps to increase security and resilience

With the above areas in mind, the following steps can help governments and cities determine their risk profile and choose the right network and communications solutions for their specific situation.

1. **Evaluate**: Identify cyber and physical risks, areas of exposure and potential consequences, as well as the different options to prevent, protect and react to attacks in each case. Start with an audit, then evaluate the risks and potential for loss for each vulnerability identified. This helps to pinpoint the appropriate actions and solutions in each case.

   While evaluation is the first step, it's not a one-time activity. To counter the fast-changing threat landscape, it's important to regularly reassess risks and continuously monitor cyber and physical resources for new vulnerabilities.

2. **Prevent**: Choose solutions that help avoid, or contain, cyber and physical risks such as:
   - From a cyber perspective, look for solutions with built-in security features that don't need to be purchased separately or renewed. Solutions should take security into account during each step of product definition, development and delivery, and contribute to a zero trust architecture and technology environment. They should also support automated backup and recovery and provide information for audit purposes.
   - From a physical perspective, identify solutions that increase visibility and make it more difficult to access assets. Solutions for video surveillance, access control, asset tracking, intrusion detection and alarms, location-based services and facial recognition are all good examples.
3. **Protect**: Choose solutions that help protect against cyber and physical risks, for example:
   - On the cyber side, ensure solutions are certified to meet security standards, include native encryption capabilities and advanced authentication mechanisms, and limit propagation of cyberattacks and viruses
   - To increase physical protection, look beyond video surveillance to consider the role of communications, alerts and notifications as well as solutions to protect workers in isolated locations
4. **React**: Choose solutions that enable efficient recovery in case of a security breach, for example:
   - Cyber solutions should be supported by a Product Security Incident Response Team, provide an audit trail and recovery procedures, and support data restoration
   - Physical solutions must support command and control (C2) operations and mission-critical communications.

Risk, resilience and security framework for public sector, governments and cities

	1 Evaluate	2 Prevent	3 Protect	4 React
Security	✓	✓	✓	
Resilience	✓	✓		✓
Cyber	• Risk identification • Assessment • Asset mapping • Valuation • Continuous monitoring	• Secure by design • Risk assessment/auditing • Pre-sales consulting • User training • Fraud detection • Backup procedure • Audit trail setup • Ruggedised for harsh environment • Redundancy	• Security certification • Encryption • Authentication	• PSIRT/CERT • Audit trail • Incident management • Recovery procedures • Restore
Physical	• Risk identification • Assessment • Valuation • Continuous monitoring	• Video surveillance • Access control • Asset tracking • Detection and alarm • Location-based services • Facial recognition • Redundancy	• Video surveillance • Communications • Alert and notification • Isolated workers protection	• Control and command • Mission-critical communications

Resilience and agile response mechanisms are key to thriving in the face of risks

" Resilience is more than just the ability to recover quickly. In business, resilience means dealing with adversity and shocks, and continuously adapting for growth. Truly resilient organisations don't just bounce back better; they actually thrive in hostile environments...Agility lets organisations respond in ways uniquely suited to each crisis, rather than apply one-size-fits-all, inflexible solutions."

— McKinsey & Company

Strengthen security and resilience

Governments and cities that follow the holistic approach and process recommended in the previous section have new opportunities to leverage network and communications solutions to increase security and resilience across citizens, operations, buildings and spaces.

Protecting citizen safety

With cutting-edge video surveillance solutions, government and public safety officials have real-time visibility into events and emergencies as they unfold, to significantly increase situational awareness. They can then use a public safety orchestration and workflow management platform to share that awareness and coordinate responses. Teams across government departments, agencies and locations can easily share timely contextual information and insights using the optimal combination of voice, video and text communications to enable more efficient, effective and collaborative decision-making.

Mass notifications systems can quickly alert people and processes to emergencies so they can take the appropriate actions faster. Calls from officials in the field have priority routing into government contact centres, and call preservation capabilities keep officials and citizens connected to contact centre staff in all circumstances. Communications solutions for lone workers, man-down situations and contact tracing further accelerate responses and increase awareness of potentially dangerous situations.

To help prevent emergencies and accelerate responses, AI solutions that are connected to multiple data sources can be used to identify risks and potentially troublesome events, and to automate workflows.

Increasing reliability across operations

A secure and resilient enterprise network supports mission-critical communications as well as the IoT, cyber and physical security technologies that are essential for reliable operations.

The ideal network solutions include features that are key to protecting access to the network and the information it carries, including:

- **Hardened source code and software on network switches**: Source code is deliberately varied to make it much more challenging for potential attackers to exploit vulnerabilities. In addition, the code and software are independently verified and validated to ensure their integrity and security.
- **Macro- and micro-segmentation**: In the context of zero trust, segmentation receives special attention at both the macro and micro levels. Macro-segmentation divides the network into distinct zones based on factors such as function, application, or user group, to isolate critical assets and resources from the rest of the network. Micro-segmentation takes a more granular approach, segmenting the network at the user or device level to enable finer control over network access and security policy enforcement.
- **Autonomous operations**: Automating the placement of assets and resources into macro-segments and applying policies at the user and device level helps reduce the risk of human errors, a common cause of cybersecurity breaches.
- **Ruggedised equipment**: Network equipment can withstand harsh conditions such as extreme temperatures and severe vibrations. Equipment supports power redundancy from two sources to ensure continuous operations during power outages. High mean time between failures (MTBF) can ensure reliability, minimising unexpected downtime and disruptions caused by breakdowns and failures.

Governments and cities also gain the flexibility to deploy network and communications solutions on premises as well as in public and private cloud environments. These deployment options enable geographic and spatial redundancy strategies that are key to maintaining business continuity during failures and emergencies, even at remote sites.

Increasing safety and security in buildings and spaces

A secure multiservice network is required to support the applications and processes needed to protect against risks and maintain service availability at all times, Additionally, to support the growing number of wireless devices connected to the Wi-Fi network, governments and cities will need a robust and reliable wireless network that operates smoothly without congestion that could lower its efficiency.

The same advanced video surveillance solutions that help protect citizens also help keep government buildings and spaces safe. These solutions are complemented with asset tracking that makes it faster and easier to find people and critical assets during unexpected events and emergencies.

Governments and cities now also have the automation capabilities required to efficiently implement and manage IoT solutions for safety and security applications, such as access control and asset tracking. They can securely and automatically onboard large numbers of new IoT devices with device fingerprinting, classification and containerisation without the risk that distracted IT personnel will inadvertently introduce vulnerabilities.

A partner to support your strategies

As the risks to governments and cities continues to grow, so does the need for an expert technology partner.

Alcatel-Lucent Enterprise, a technology innovator for more than 100 years, has developed a Risk, Resilience and Security (RRS) framework that aligns with government and city requirements. The RRS framework includes the processes, best practices and solutions governments and cities need to predict, monitor, avoid and counter exposure to cyber and physical risks.

The ALE team of highly knowledgeable government specialists, partner with government and city leaders to help:

- Identify their unique set of risks and choose solutions to address the risks
- Bridge the gaps between cyber and physical security, and resilience
- Make the case for budget approvals

Flexible, fully compliant solutions

ALE embeds security into its network and communications solutions from the earliest stages of design. To ensure maximum security and resilience, the solutions:

- Are built with security measures trusted by governments and defence organisations around the world
- Are tested using specialised, security-specific techniques, such as penetration tests
- Comply with global, industry-specific and regional data security and privacy standards, including key security industry standards, such as Common Criteria EAL2+
- Can be deployed in any combination of on premises and cloud models to meet the most complex requirements
- Support open standards to reduce integration complexities and incompatibilities across solutions and vendors

In addition to traditional purchase models, ALE offers subscription plans so customers can access the latest technologies and security advances while meeting budget constraints. A complete suite of services to support governments and cities at each stage of their journey is also available.

Experience + expertise

ALE experts and solutions are trusted by government and city organisations around the world. Following are just a few examples:

- Metz Eurometropolis in France, where ALE helped the metropolitan area ensure continuity of critical services and communications, quickly make emergency services available, and securely link users and connected objects across buildings.
- The Scottish Government, where ALE solutions provide consistent, secure and reliable infrastructure and network access control, as well as enhanced data security, for more than 40 government agencies.
- The U.S. Department of Defense, where ruggedised, modern solutions reliably support mission-critical communications and applications while meeting all environmental and shock requirements, as well as Trade Agreement Act (TAA) and defence certification requirements.
- Gwinnett County Public Schools in the U.S., where ALE solutions support physical security, video monitoring, E-911, secure computing and more in a large school district where safety and security are paramount.

Learn more

To learn how Alcatel-Lucent Enterprise can help your organisation mitigate risks to increase security and resilience, visit website or contact us today.

Alcatel·Lucent Enterprise