CYBER RESILIENCY FRAMEWORK

Cyber Resiliency relates to a city's ability to deliver services at all times, knowing the threat landscape, and in case of an event having the ability to bounce back and resume normal operations. This framework is a collaboration between the Chief Information Security Officers (CISOs) of the District of Columbia, New York City, San Francisco, and The Hague.

Why Now?

Malware attacks on the web increased 23% in 2013 and on mobile devices 139% in the same period.

Online attacks claim 1.5 million victims every day, conservatively $110B in losses every year.

By the Year 2020, there will be 50 billion smart objects and a population of 7.83 billion people.

Per Gartner, by 2020, companies will spend about $170B on Cybersecurity.

Framework Domains

The following 5 domains lay the foundation for a Cyber Resiliency Framework. They must individually and collectively influence the city's smart city vision, strategy, and deployment.

GOVERNANCE

You must inspire the greatest participation within the city and between cities to achieve a smarter city.

City Governance — Your government must connect internally with its own agencies, the community, industry, and research institutions.

Technical Governance — Technologies must be designed, developed, and deployed in a framework that promotes consistency, interoperability, and is secure.

SURVIVABILITY

Critical infrastructure cannot rely on fragile communications systems or those at high-risk of failure during major incidents.

Redundancy — Ensure all critical systems have alternate or backup capabilities.

Service Prioritization — Prioritize services and allocate resources to meet demands in an emergency.

Cyber Protection — Design and deploy effective cyber protection into all systems.

Wireless Vulnerabilities — Deploy adaptive IoT devices built to resist interference or have alternate communications routes.

Environmental Sturdiness — Deploy environmentally rugged devices able to operate in extreme conditions.

Continuity Plan — Develop a plan to minimize impacts if a catastrophe occurs.

DEVICE PRIORITIZATION

The enormous growth of connected devices provides opportunity for new services but must be effectively planned and managed.

Device / Service Classification — Each device and service needs to be classified to aid in prioritization.

Quality of Service (QoS) / Priority — Your networks should have the capability to give priority to the most critical devices during an emergency.

Identity Protection Management — Provide a strong authentication solution to protect digital assets.

DATA & PRIVACY

Data is extremely valuable in how cities today operate and must be managed and protected accordingly.

Data Architecture — City data should adhere to standards that allow easy and interoperable use.

Data Classification — Data should be classified as public data or private data to determine how data should be protected, utilized, and by whom.

Data Protection — Data security standards are needed to protect and monitor for abuse, misuse, and unauthorized access.

Data Privacy and City Transparency — There must be a reasonable expectation of privacy to maximize adoption of innovative technologies.

EDUCATION

Effectively educate executives, citizens, and technology professionals to drive adoption.

City Executives — Create an understanding of the actual, often unknown, cyber risks and how government can manage these risks.

Public Safety Professionals — Give visibility into how their agencies can function more effectively and cost-efficiently.

Citizens — Inform and train citizens about how to communicate and problem solve during a major incident.

Technology Professionals — Provide new, multi-disciplinary training to educate professionals on how safety and security professionals operate.

WE ARE WASHINGTON DC

NYC

THE CITY AND COUNTY OF SAN FRANCISCO

VREDE EN RECHT

The Hague