Cybersecurity in Next Generation 911 (NG911)

PROTECTING EMERGENCY COMMUNICATION SYSTEMS

BRITISH COLUMBIA

Matthew Golshani
Ivan Rincon
Ministry of Citizens' Services

What is Cybersecurity?

THE COST TO REMEDIATE A CYBERATTACK FAR EXCEEDS THE COST OF PREVENTING ONE

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks.

It involves implementing measures to safeguard sensitive information and ensuring the confidentiality, integrity, and availability of data across various digital and cloud platforms.

Key aspects include:

- **CIA Triad –** Confidentiality, Integrity, and Availability.
- **Security First Principle –** The prioritization of security at every stage, make security proactive.
- **Risk Management –** Cybersecurity is fundamentally about managing risk. Following good risk management strategies allows for effective prioritization of security efforts on potential threats.

CONFIDENTIALITY

Is concerned with ensuring data is only accessible by individuals or systems that are authorized to do so.

INTEGRITY

Is concerned with ensuring data remains accurate, consistent, and unaltered during transmission or storage.

AVAILABILITY

Is concerned with ensuring data is accessible and available to authorized users when needed.

Security First Principle

ENSURING RESILIENCE AND SECURITY THROUGHOUT EVERY STAGE OF DEVELOPMENT AND DEPLOYMENT

A security first approach prioritizes security at each stage of development, system design, and operation. Making security proactive rather than reactive will ensure systems are always resilient and defensible.

Key concepts include:

- Principle of least privilege
- Defensive in depth
- Risk based approach

Cybersecurity Threat Landscape

COMMON SECURITY THREATS

- Malware
- Phishing
- Denial of Service attacks (DDoS)
- Insider threats (social engineering)
- Zero-day exploits

CONCERNS WITH CYBERATTACKS

- Cyberattacks are constantly getting more complex and sophisticated, increasing the difficulty of keeping systems and data secure.
- The cost of breaches can potentially cost millions of dollars, destroy applications, and steal sensitive data.
- A strong understanding of threats and vulnerabilities is needed to effectively combat cyberattacks.

Why Cybersecurity Matters in Public Safety

PROTECTING EMERGENCY SERVICES

Cyberattacks on emergency services and dispatch centres can delay response times or even block access, putting the publics safety at risk.

It is imperative that all public safety systems comply with relevant cybersecurity regulations and requirements to keep people safe.

Emergency services handle personal and medical data of the general public, a data breach can put people at risk and expose victims or even first responders.

Threat Concerns:

- **Ransomware attacks** – can cripple communications blocking access to essential systems.
- **Social engineering** – can allow attackers to gain access to internal systems and data.
- **Malware infections** – such as trojans or worms can cause slowdowns in response times or even shut down systems completely causing a loss of emergency services for populated areas.
- **DDoS attacks** – can overwhelm an emergency services system causing a loss of available service to the public.

Why is Cybersecurity critical in NG911?

Next-Gen 911 (NG911) Overview

A MODERN APPROACH

NG911 is a modernized, IP-based emergency response system set to replace our current landline based infrastructure.

- **The IP-based system –** enables faster and more efficient communication through the following improved features:
- **Voice, text, imaging, and video capabilities –** allow a much more comprehensive level of communication between the general public and Public safety access points (PSAPs).
- **Enhanced location accuracy –** GiS mapping and GPS tracking allows PSAP call takers and dispatch services to see callers location in real-time assisting in faster and more reliable help from emergency services.
- **Improved data sharing –** An IP-based system allows for more comprehensive information be shared with the relevant dispatch service, improving 911 wait times and first responders readiness when arriving on scene.

Why Cybersecurity Is Critical For NG911

A SECURE NG911 ENSURES SAFE & RELIABLE EMERGENCY RESPONSE

NG911 relies on interconnected digital networks making it an easier target for cyber threats and attacks.

- Increased access and availability of 911 services also means an increase to the vulnerability and risk of cyberattacks on the NG911 ecosystem
- The importance of having strong cybersecurity standards and requirements implemented is far greater in a IP-based system to ensure threat actors cannot compromise critical emergency services

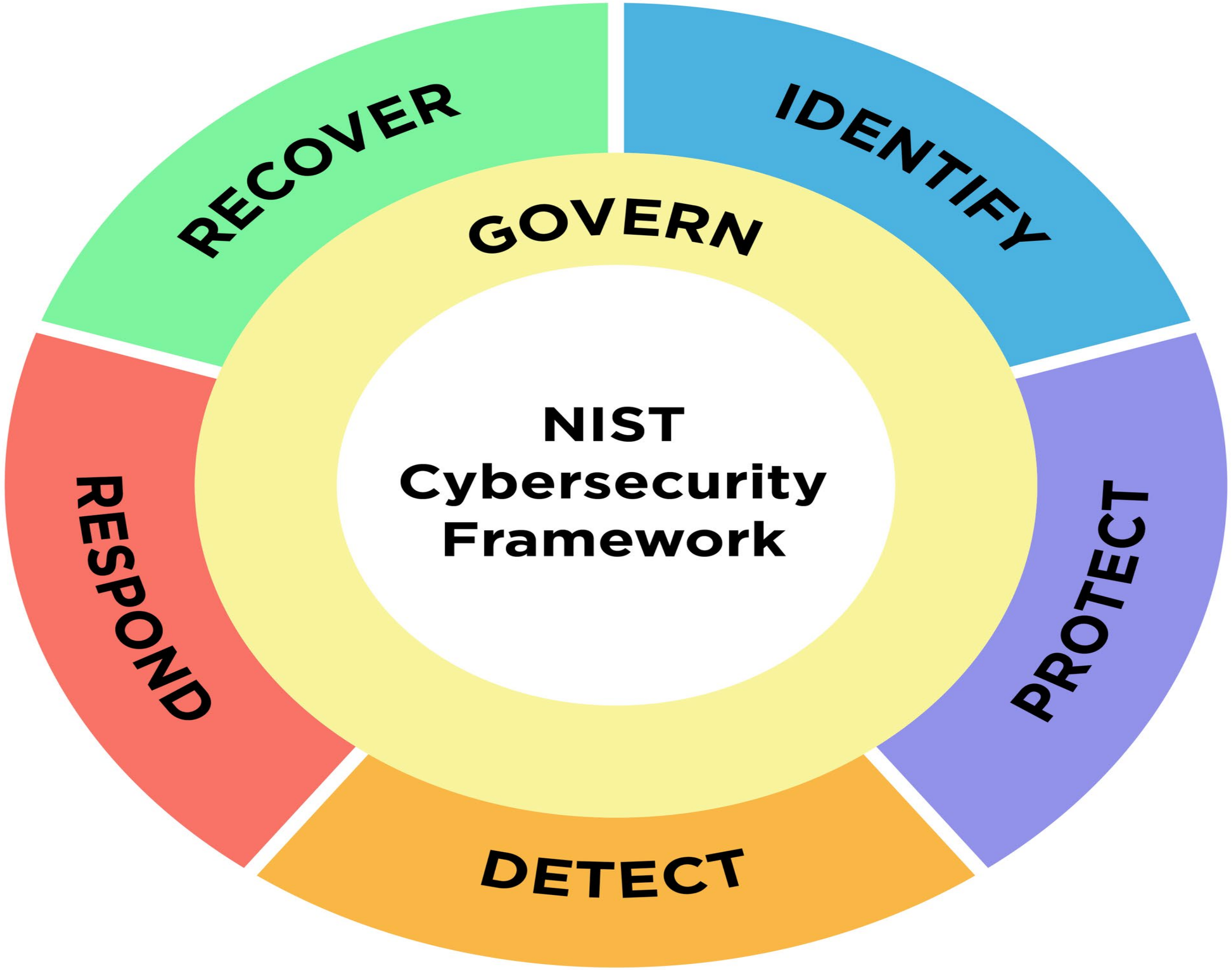
Security challenges of NG911 vs E-911

Being an IP-based system creates new risks of cyberattacks on the 911 infrastructure.

- DDoS, ransomware, and data breaches are all risks that need to be addressed in the new ecosystem.
- NG911 transmits real-time location data, medical history, and multimedia making it a high-value target for cybercriminals.
- With the addition of text and video capabilities in the new system there is an increase to the entry points for potential attacks.

Implementing NG911 requires strict adherence to cybersecurity standards and continuous updating and monitoring to ensure the confidentiality, integrity, and availability of emergency services.

Implementing cybersecurity standards in NG911



NIST 2.0 is a framework designed to help organizations manage and reduce security risks.

NENA Standard for NG911 Implementation

NATIONAL EMERGENCY NUMBER ASSOCIATION (NENA)

NENA standards are based on the NIST 2.0 framework and set the requirements that all PSAPs must adhere to in the implementation of NG911s infrastructure.

These standards ensure that cybersecurity best practice are followed to keep NG911 secure, and accessible.

Key security measures for NG911 & NENA compliance:

- **Network security** – Prevents DDoS attacks and unauthorized system access.
- **Data security** – Prevents data breaches, unauthorized leaks and compliance violations.
- **Access controls & Authentication** – Prevents insider threats, phishing attacks, and unauthorized data modifications.

Training & Awareness For NG911 Security

NG911 systems handle critical emergency communications – a single cyberattack can disrupt 911 services, delay response times, and put lives at risk. Training PSAP personnel, IT teams, and first responders is essential to maintaining a secure and resilient system.

Key areas of training for PSAP personnel include:

CYBER THREAT AWARENESS

Phishing scams and social engineering identifying ransomware / DoS threats, understanding insider threats and access control risks.

SECURE SYSTEM OPERATIONS

Proper use of authentication including multi-factor authentication (MFA), proper handling of sensitive data, following NENA security guidelines for system access.

INCIDENT RESPONSE & RECOVERY

What to do in the event of a cyberattack, reporting suspicious activity, active cyber drills and exercises.

Why Training Is Essential For NG911

MOST CYBERATTACKS CAN BE MITIGATED THROUGH WELL TRAINED PERSONNEL

Well trained PSAP staff will ensure the essential emergency services of NG911 are available for the sake of public safety.

Key outcomes of cyber awareness training:

- **Prevents human error –** reduces the risk of phishing scams and giving unauthorized access to attackers.
- **Strengthens incident response –** responding quickly to a threat actor is essential to reducing the severity of the attack.
- **Enhances system resilience –** ensures a broader, more comprehensive level of security & system availability.
- **Ensures compliance –** Properly trained personnel is one of the requirements of effectively adhering to NENA standards.

The Future of Cybersecurity

AS NG911 EVOLVES, SO DO CYBERTHREATS

Emerging technologies and government initiatives are necessary to shaping a more secure and safe future for 911 call centres.

With modern day advancements in computing and AI, the need to stay up to date on new technologies has never been greater. Machine learning models and cloud-based infrastructure are the inevitable future of technology.

Finding a secure and safe way to utilize new technologies will be essential in the future of cybersecurity & NG911.

Resources & References

National Institute of Standards and Technology (NIST)

National Emergency Number Association (NENA)

Next Generation 911 - Province of British Columbia

NG911 GeoHub

911 Cybersecurity Resource Hub | CISA

Q&A - closing remarks

Thank you

BRITISH
COLUMBIA