



The Impact of Cyber Attacks on Law Enforcement Agencies

Law enforcement agencies, big and small, around the world are increasingly victims of ransomware attacks. Criminal hackers are utilizing brazen tactics to infiltrate networks with threats to leak highly sensitive and potentially life-threatening information without fear of repercussions.

Every 11 seconds, a ransomware attack occurs.

Ransomware is a “threat to national security” – *Alejandro Majorkas, Homeland Security Secretary.*

This should be a wake-up call to law enforcement agencies that they need to take strong and decisive action.

To learn more about how **Telos Ghost**® can help to protect your critical assets, visit www.telos.com/telos-ghost or contact us: inside.salesteam@telos.com

Washington Metro Police Department

250 gigabytes

of data stolen, with threats of release of information on police informants to criminal gangs if ransom was not paid in three days.

Trenton Police Department

2x in 6 months

ransomware attacks caused the Trenton Police Department to lose all data. There was no backup.

Tulsa Police Department

18,000

files exposed, including police citations and internal department files containing PII such as names, birth dates, addresses, and driver's license numbers.

Los Angeles Police Department

20,000

records impacted by a data breach, including names, birth dates, email addresses and passwords, and partial social security numbers.

Azusa Police Department

Payroll records

stolen, including social security, driver's license, and passport numbers and financial and medical information.

Baltimore Dispatch

17 months

of 911 and emergency dispatch system disruption due to a cyber breach.

