Emergency Services – Protecting, the Command & Control
Case Study – Emergency Services Telecommunications & Command Centers

The Client

A Government agency responsible for directing and running a major city's Emergency Services Telecommunications.

A Government agency responsible for running the Emergency Services Telecommunications of one of the world's largest multi-agency emergency services zones, handling more than 1.8 million emergency calls a year. Representing a call every 16 seconds, leading to more than 1,200,000 dispatches requiring an emergency response.

The Government agency in partnership with its public safety, technology provider is responsible for managing emergency calls and associated operational communications for dispatching police, fire, ambulance and State Emergency Services - 24x7, covering some 5 million citizens. In addition, to coordinating emergency radio, paging and mobile data communications for the emergency services.

CYBERRISK.COM
SECURITY - ASSURANCE - FORENSICS - ENABLING

The Challenge

A serious cyber attack against networks - breaching data, privacy and damaging IT equipment. The immediate challenge called for rapidly assessing and containing the incident and carry out a detailed forensic investigation.

The forensic investigation had to be allied with a comprehensive integrated security review and cyber risk assessment of the emergency services Computer Aided Dispatch (CAD) platform and the command and control centres.

Response

Cyberrisk.com was engaged as a strategic partner. Leading the cyber and physical security review of the mission critical CAD platform and the command and control centres. In addition to applying our computer network and malware forensic capabilities as part of the cyber attack forensic investigation.

Cyberrisk.com carried out detailed threat modelling, vulnerability and risk assessments, code reviews and penetration testing. As always our aim is to provide an integrated security solution, premised on our risk based approach to cyber security. Thereby ensuring the seamless protection of the entire security ecosystem, driven from the boardroom but owned by all in the organisation. A successful cyber risk awareness and education program was carried out as well.

Result

- The source of the cyber attack attributed and successfully prosecuted
- Rapid remedial action prevented further data breaches and privacy losses
- Development of a robust integrated security strategy and vulnerabilities mitigated
- The provision of tailored cyber risk intelligence and risk visualisation support
- Continuous cyber risk and cyber security training
- Adoption of "Data Centric Security" and "Privacy by Design" as embedded principles in the organisation
- Cyber Risk Management adopted as a core tenant of overall enterprise risk management and represented on the board

e-mail: hi@cyberrisk.com