SOLACOM

CYBERSECURITY: 3 STEPS EVERY PSAP SHOULD TAKE TO REDUCE RISKS

With the move to IP-based Next Generation 9-1-1 (NG9-1-1) emergency call handling systems, new cybersecurity threats are emerging. And business continuity plans must be updated.

Follow these three steps to reduce the risks that cyberattacks pose to your organization.

1 Increase Understanding

- **Network infrastructure and connection threats:**
  - Denial-of-service (DoS)
  - Telephony DoS (TDoS)
  - Man-in-the-middle
- **User and device threats:**
  - Ransomware
  - Data breaches
  - Malware
- **Operations threats:**
  - Swatting

2 Evaluate Requirements

Explore cybersecurity strategies and solutions from two perspectives:

- **Network perspective:**
  - Prevent unauthorized access
  - Recognize signs and symptoms
  - Escalate response levels
  - Contain the spread of attacks
  - Mitigate against future attacks
- **On-premises perspective:**
  - Schedule upgrades and patches
  - Minimize open connections
  - Set up backup sites
  - Develop policies and training
  - Authenticate all users

3 Engage Experts

Talk to NG9-1-1 cybersecurity experts about:

- Factory-installed protection capabilities in NG9-1-1 systems
- Active remote monitoring of NG9-1-1 systems
- Disaster recovery services
- Firewalls and session border controllers (SBCs)
- Server hardening and workstation lockdown

Position Your PSAP for a Secure Future With Solacom

Solacom understands the security requirements in NG9-1-1 systems. Our call handling and management solutions are built on more than 30 years of research and innovation. And we provide a complete suite of managed services that help PSAPs reduce the risks associated with cyberattacks.

Find out why Solacom is the choice of leading PSAPs and state and local governments.

www.solacom.com