ICU
MANAGEMENT & PRACTICE

Cyber Security and Emergency Medical Systems: going beyond ‘Patch and Pray’

Recent cyberattacks have left public authorities reeling at the relative ease with which a malign individual or organisation can bring about widespread disruption of services. The main target of recent attacks in the health sector was the National Health Service in the UK. The fact that the problem boiled down to a software fix or ‘patch’ which had not been applied to an outdated operating system, must serve as a major wake-up call to public health authorities across Europe.

Whilst the attacks caused much disruption, so far, fortunately, this has not translated into loss of life. The scenario could have been far more serious. Imagine, for example, a cyberattack on emergency medical services, and - in the worst case - timed to coincide with a physical attack requiring a major emergency response.

The problem of cyberattacks is therefore not just about security and privacy or patient data. There are multiple areas of concern as communications, information systems, medical and monitoring devices are increasingly interconnected. Patient safety could be severely compromised through:

- mis-directed or no emergency medical dispatches and slower overall response times.
- corruption or unauthorised manipulation of data, disruption or difficulty accessing information on which operational and clinical decisions are made, and failure to receive or send critical alerts.
- lack of confidence in data integrity, leading to confusion amongst first responders, emergency dispatch centres, physicians and medical teams in hospitals.

Despite differences in laws and regulations in different EU Member states, the underlying challenges are similar. Steps are being taken to improve cyber security at a system-wide level, for example through the 2013 EU Cyber Security Strategy, the 2015 Digital Single Market strategy, and the 2016 EU Directive on security of network and information systems.

However there is still little attention to the specific challenges of emergency medical response in the event of cyberattacks. A coordinated, proactive approach is needed to mitigate and respond to these threats. Specifically, we call for:

- a pan-European risk assessment of cyber threats to emergency medical systems, not limited to the pre-hospital environment, but also considering the implications for in-hospital teams.
- promotion of resilience activities and contingency planning
- a road map for embedding cyber security into emergency response systems, the design and development of networked medical and monitoring devices, and improvements in governance and accountability for cyber security in healthcare settings.

As data becomes more and more essential to healthcare delivery, data security – encryption, data transfer and storage – are increasingly being factored into service planning and development. However this requires the right level of attention and resourcing from the initial design through delivery and deployment. In the meantime, urgent efforts are needed to understand and assess the extent of cyber vulnerabilities so that vital clinical systems can be securely ring-fenced to allow them to continue to function safely and effectively should similar attacks happen in future.

Source Credit: **European Critical Care Foundation**
Image Credit: **freeimages.com**

Published on : Wed, 24 May 2017