HealthManagement
Promoting Management and Leadership

Strengthening Cybersecurity in European Healthcare

The European healthcare sector is facing an unprecedented rise in cyber threats, with hospitals and medical providers becoming prime targets for cybercriminals. The increasing reliance on digital health solutions, electronic health records and connected medical devices has expanded the sector's exposure to cyberattacks. These attacks disrupt essential medical services, delay treatments and compromise patient safety. The European Commission has recognised the urgency of this situation, developing a comprehensive action plan aimed at enhancing cybersecurity resilience in hospitals and healthcare providers. The plan prioritises a structured approach focusing on prevention, detection and response to cyber threats. Strengthening cybersecurity across the sector is essential to maintaining trust in healthcare systems and ensuring the uninterrupted delivery of patient care.

The Rising Cyber Threats to Healthcare

Cyber threats targeting healthcare organisations are becoming more sophisticated, with ransomware attacks emerging as the most significant concern. Criminals exploit weaknesses in hospital IT systems, encrypting critical patient data and demanding ransom payments for its release. Beyond financial motives, some attacks have a geopolitical dimension, with state-backed actors targeting healthcare infrastructure as part of broader cyber warfare strategies. The consequences of such attacks are severe, leading to operational disruptions, delays in medical procedures and, in extreme cases, life-threatening situations.

The COVID-19 pandemic underscored the vulnerability of healthcare institutions, as hospitals and medical research facilities became prime targets for cyberattacks. The high value of health data, including patient records and medical research findings, makes the sector an attractive target for both financially and ideologically motivated actors. The widespread adoption of digital health tools and cloud-based systems has further increased the attack surface, requiring more robust cybersecurity measures.

Medical devices, including those connected to the internet, pose another significant risk. Many devices lack adequate security protections, making them potential entry points for cybercriminals. A security breach in one device could have cascading effects across an entire healthcare network. The growing complexity of hospital IT infrastructure also presents challenges in maintaining security across multiple interconnected systems. With hospitals relying on various suppliers for IT solutions, electronic health records and cybersecurity services, weaknesses in third-party vendors further compound the sector's vulnerabilities.

Enhancing Cybersecurity Maturity in Healthcare

The cybersecurity maturity of healthcare institutions varies widely across Europe, with many hospitals struggling to implement even basic security measures. A lack of dedicated cybersecurity personnel, insufficient risk assessments and reliance on outdated IT infrastructure contribute to vulnerabilities in the sector. Smaller healthcare facilities, in particular, face resource constraints that limit their ability to invest in cybersecurity measures. Many organisations continue to use legacy systems that are difficult to upgrade, leaving them exposed to known security flaws.

The European Commission's action plan aims to address these gaps by fostering a culture of cybersecurity awareness among healthcare professionals. A crucial element of this initiative is the development of cybersecurity maturity assessments, which will help hospitals evaluate their security posture and identify areas for improvement. Training programmes tailored for healthcare providers are also essential to ensure staff are equipped with the knowledge to recognise and prevent cyber threats. Human error remains a major contributor to security breaches, with phishing emails and weak authentication practices being common attack vectors. Raising awareness of these risks and implementing strong cyber hygiene practices can significantly reduce vulnerabilities.

Another key measure proposed in the action plan is the implementation of sector-wide cybersecurity guidelines. These guidelines will help standardise best practices and provide clear recommendations for improving security in healthcare settings. Hospitals will be encouraged to adopt essential measures such as multi-factor authentication, encrypted data storage and continuous monitoring of network activity. Strengthening security at all levels, from frontline staff to IT administrators, is critical in reducing the risk of cyber incidents.

The Role of a Coordinated European Response

Cyber threats are not confined to national borders, making a coordinated EU-wide approach essential. The European Commission's action plan includes the establishment of a European Cybersecurity Support Centre specifically for hospitals and healthcare providers. This centre will serve as a focal point for cybersecurity expertise, facilitating knowledge-sharing, issuing security guidance and coordinating responses to cyber incidents. By consolidating resources at the EU level, the centre aims to improve the overall resilience of the healthcare sector.

A critical component of the action plan is the enhancement of early threat detection capabilities. The introduction of a Europe-wide early warning system will enable healthcare institutions to identify and respond to emerging threats more effectively. Information-sharing networks, such as the European Health Information Sharing and Analysis Centre (ISAC), will play a crucial role in fostering collaboration among hospitals, cybersecurity experts and national authorities. Timely access to threat intelligence can help healthcare organisations take proactive measures to mitigate risks before they escalate into major incidents.

In addition to preventive measures, the action plan outlines steps for improving incident response and recovery. The EU Cybersecurity Reserve will be mobilised to provide rapid support in the event of a significant cyberattack, ensuring that affected hospitals receive the necessary technical assistance. Cyber incident response playbooks will also be developed to guide healthcare institutions in managing security breaches effectively. These structured response plans will help hospitals contain cyber incidents, minimise damage and restore normal operations as quickly as possible.

As healthcare systems become increasingly reliant on digital technologies, cybersecurity must be prioritised as a fundamental aspect of patient safety and service continuity. The European Commission's action plan provides a structured and comprehensive approach to addressing cyber threats in the healthcare sector, with a focus on prevention, detection and incident response. However, its success will depend on the commitment of hospitals, national authorities and private sector stakeholders to implement these strategies effectively.

Investment in cybersecurity infrastructure, workforce training and coordinated threat intelligence sharing will be essential to building a more resilient healthcare sector. As cyber threats continue to evolve, healthcare institutions must remain vigilant and proactive in defending against emerging risks. Strengthening cybersecurity across hospitals and healthcare providers is not only a technical necessity but also a critical safeguard for public health and trust in medical institutions.

Source: **European Commission**

Image Credit: **iStock**

Published on : Tue, 4 Feb 2025