Cybersecurity in Healthcare: A Call to Action

Tony Chebli
CEO, ANAT Security
Paris, France

In October 2025, I was invited to a conference by the Lebanese Society for Quality and Safety in Healthcare (LSQSH) to speak about cybersecurity attacks and how to detect them in hospitals. This marked my first experience addressing the healthcare industry, a significant shift from my usual analogies between data and the human body. On that day, I focused on something even more critical than financial data: the well-being and safety of patients.

I began my presentation with a case study of a mid-sized hospital outside Lebanon that fell victim to a ransomware attack. As I detailed how the attack unfolded, I highlighted the moment when hospital management realized they were compromised. **Ransomware—a form of malicious software that restricts access to data until a ransom is paid—is becoming an increasingly significant threat in the healthcare sector**, which is often viewed as low-hanging fruit. Attackers typically encrypt vital patient data, leaving hospitals paralyzed and demanding payment for its return.

I concluded my presentation by emphasizing that hospitals must acknowledge the likelihood of a cyberattack occurring at some point. To effectively detect incidents, hospitals should follow established frameworks such as ISO 27035 for incident management and the NIST Cybersecurity Framework (NIST SP 800-61), which provide structured approaches to managing and mitigating cybersecurity risks.

The subsequent sessions of the event revealed that some Lebanese hospitals have indeed been targeted by cybercriminals, with one hospital suffering from multiple ransomware attacks. Unfortunately, neither presenter could provide details on how these breaches occurred due to the absence of essential logs—an unfortunate yet common tactic employed by professional hackers to cover their tracks. In the absence of these logs, understanding the specifics of the hacking becomes speculative, complicating efforts to identify effective preventive measures for future incidents. This scenario highlights an important distinction: consultants offer subjective opinions, while audits provide factual assessments.

As a definition, ransomware attacks, fundamentally motivated by financial gain, are typically signaled by a message demanding payment to unlock the compromised systems. In the cases we discussed, the hospitals chose not to pay the ransom, resulting in prolonged operational disruptions lasting weeks or even months as they worked to recover.

It is also important to consider the potential repercussions of paying a ransom, including severe sanctions from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). Organizations that engage with sanctioned individuals or entities risk being placed on the OFAC list, facing legal and financial consequences.
Moreover, attackers often escalate their threats by contacting directly the patients of affected hospitals, warning them that their data may be exposed if the relevant hospital does not pay the ransom.

The two hospitals managed to recover from their attacks using a bottom-up approach, focusing on local and external IT teams to address immediate issues. However, I recommend adopting a top-down approach to information security. This strategy emphasizes leadership involvement and fosters a culture of security throughout the organization. While ransomware is a significant threat, it is far from the only concern. Hospitals also face various cyberattacks, including phishing attacks, denial-of-service (DoS) attacks, and data breaches, many of which often remain unreported. Notably, a study conducted by Cisco found that 80% of organizations need to take action to improve their cybersecurity measures. Additionally, another report indicates that nearly 80% of German companies experienced incidents related to data theft, industrial espionage, or sabotage within the last 12 months.

Utilizing international standards such as ISO 27001, which encompasses people, processes, and technology, can assist hospitals in creating a comprehensive security framework. This framework should not only protect data but also ensure that patient privacy is effectively addressed. **Integrating privacy considerations into security measures is essential for building trust and safeguarding sensitive information.**

In conclusion, the urgency of addressing cybersecurity threats in the healthcare sector cannot be overstated. As we move forward, hospitals must prioritize their cybersecurity frameworks, acknowledge the reality of cyber threats, and take proactive measures to protect patient data and safety. By embracing both top-down and bottom-up approaches and adhering to international standards, we can better prepare for and respond to the challenges ahead.
The journey toward robust cybersecurity in healthcare requires commitment, vigilance, and a collaborative approach. Together, we can ensure that our healthcare systems remain resilient against the ever-evolving landscape of cyber threats.