Over the past few decades, the healthcare sector has relied more and more upon technology. From the use of AI and machine learning models to electronic prescriptions and pharmacy management, the heavier reliance on technology also requires a higher emphasis on cybersecurity.

Last year the ransomware attacks on the healthcare sector nearly doubled. Unfortunately, there is worse to come as the current global damage from ransomware of £20 billion per year is expected to rise to £265 billion a year by 2031. Specific to healthcare, 66% of cyberattacks disrupt patients care, yielding significant increase in medical complications in 50% of the cases and mortality rates in 23% of the cases. Considering that at least 1 out of 40 hospitals were hit by a cyberattack in 2024 alone, this means governing and overseeing cyber risk becomes an essential component to drive patient care. Unfortunately, organizations often seem to underestimate the non-technical consequences of cyber threats. Our research shows that cyber risk is not easy to understand. Advancing patient care, operational, and financial alignment to cyber risk management as well as having a sectoral overview are essential.

Managing cyber risk through a medical lens is important. From a board perspective, cyber security should be a top priority because of its susceptibility to cyberattacks. Firstly, a board must understand that poor cyber defense carries an implicit cost of life. In the face of a ransomware attack where crucial patient data is compromised, doctors cannot make correct diagnosis and prescriptions. In 2020, a cyberattack against a hospital in Germany led to disabled IT services and no access to patient care services. As a result, a woman in need of urgent care was forced to be redirected to another hospital 20 miles away, where she passed away en route.

Secondly, boards must be able to find ways to mitigate the risk of having interconnected network environments. The healthcare sector commonly uses integrated systems for electronic health records, patient records, billings, and diagnostics. As a result, any ransomware attack can easily spread throughout multiple networks, making an already tough situation even worse.

Thirdly, and perhaps most importantly, a ransomware attack that compromises a hospital leads to cascading effects across all hospitals near the area. Diverted patients from a compromised hospital puts extreme stress on other hospitals in the region. Ambulances must take to further destinations, delaying crucial care times. ICU's, beds, and healthcare personnel at other hospitals are stretched thin, leading to higher stress and more medical mistakes. In 2020, a ransomware attack disrupted the University of Vermont Medical Center, causing patients to be redirected to other hospitals in New York and New England, causing severe strain and bottleneck effects. A similar situation happened again in 2021, where a ransomware attack on Scripps Health in San Diego forced the hospital to divert stroke and heart attack patients to nearby hospitals. Once again, this strained emergency services for healthcare services around the area and ER wait times increased significantly.

It is crucial that healthcare companies invest into cyber risk governance and critical infrastructure. Whether that's hiring a Chief Information Security Officer (CISO) to oversee a

cybersecurity team or educating the board about the dangers of a cyberattack, the healthcare industry must treat cybersecurity as an equal to physical care. **(Unsure of what else to add here…)**

On a national level, the NIST Cybersecurity Framework provides a good blueprint for how organizations should approach their cyber risk governance. It has clear sections for prevention, detection, response, and recovery that healthcare companies should at the very minimum, follow to a tee. More recently, the SEC has also tightened their guidelines for cyberattacks, including mandating the disclosure of cyberattacks and cyberdefense strategies. Although there are no specific mandates for the healthcare sector, it is generally advised that they tighten their cybersecurity defenses even more due to their especially vulnerable position and their management of people's lives.

However, it is no secret that managing cybersecurity can be expensive and confusing. It's hard to determine the optimal amount of money and resources to dedicate to cybersecurity, since it is nearly impossible to attach a monetary amount to cyberattacks that were prevented or stopped. Therefore, taking preventative measures like additional firewalls or stronger data encryption may be seen as a waste of money to healthcare boards. It only becomes clear that additional investment to cyberdefense is needed only after an attack, but by then it could be too little, too late.

But perhaps the greatest downside to cyberattacks is its long term and recurring nature. All attacks have its upfront costs, like the cost to repair and the cost of the ransom. However, there are also secondary costs that may not be recorded, like the loss of trust from patients, brand damage, the loss of functionality, increased insurance costs, etc. For instance, the Anthem Inc. data breach in 2015 resulted in $115 million in upfront costs, but after taking into account the $16 million HIPAA fine, the $31 million cost to notify individuals, $112 million for credit protection services, and combined with the loss of customer trust, the total cost came out to be well over $270 million.

The healthcare industry has also been struggling to recover after the Covid-19 pandemic. A study conducted just earlier this year revealed that more than 700 rural hospitals are at risk of closure, which represents around 30% of all rural hospitals. LA specifically was hit hard during the pandemic as rising costs and employee burnout caused around a dozen hospitals to shut down in mainly low-income and minority neighborhoods. These hospital shutdowns not only create healthcare deserts, but also puts additional strain on other medical centers around the area.

These factors mean that any cyberattack that disrupts a medical center can be catastrophic to both patients and the healthcare sector. For many hospitals, recovering from a ransomware attack by paying the ransom may be just enough to push their finances underwater. When taking into account the future costs as well, it becomes clear that cybersecurity should be a priority for the healthcare industry.

There are 3 main points that the healthcare industry must address:

1. Employee and board training
2. Dynamic and robust security infrastructure
3. Incident response plan