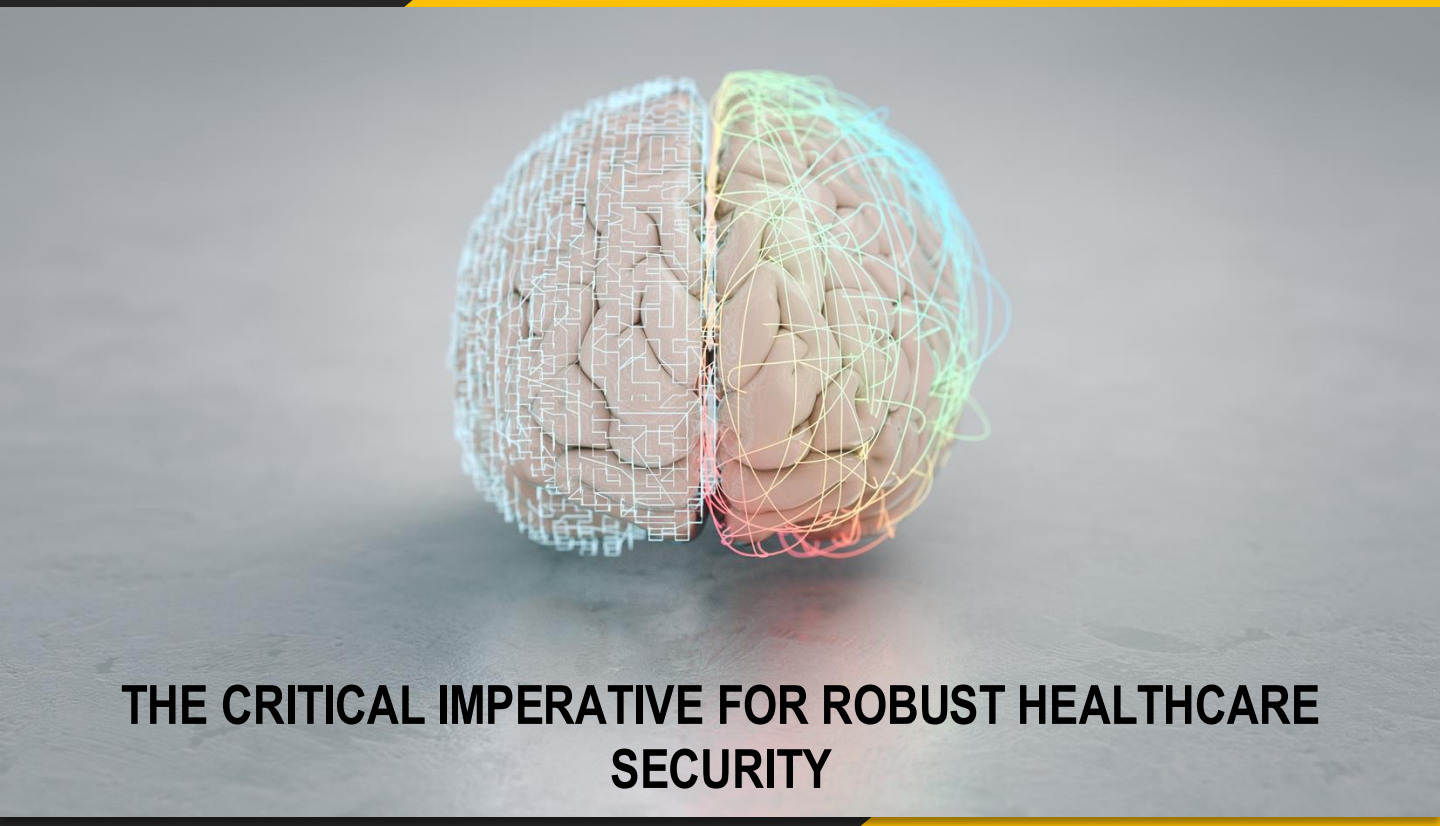
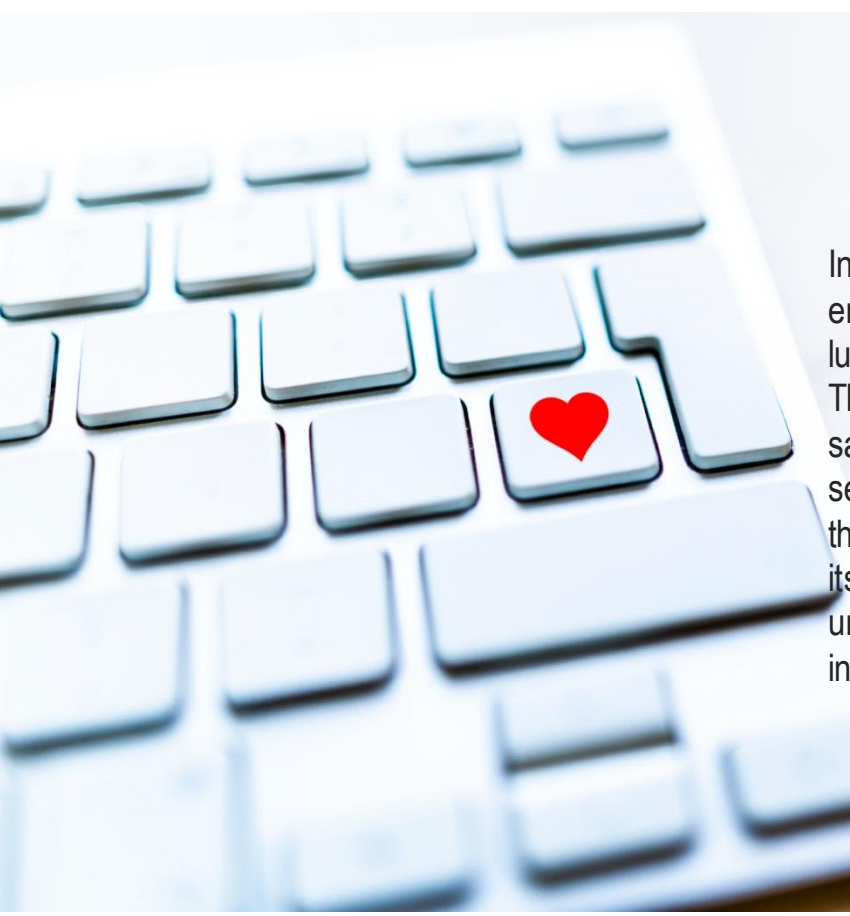
Proton Technosoft
Securing your digital footprints !!



THE CRITICAL IMPERATIVE FOR ROBUST HEALTHCARE SECURITY



In today's digitized healthcare environment, security is no longer a luxury—it's a life-and-death necessity. The healthcare sector, tasked with safeguarding some of the most sensitive personal data, has become the top target for cybercriminals due to its vast attack surface and historically underfunded cybersecurity infrastructure

Healthcare Is the #1 Target for Cyberattacks

According to IBM's Cost of a Data Breach Report 2024, the healthcare industry experienced the highest average cost of a data breach for the 13th consecutive year, at $10.93 million per incident, nearly double that of the second-ranked industry. The increasing digitization of patient records and reliance on interconnected medical devices make hospitals particularly vulnerable.

Ransomware Threats Are Rising Exponentially

A report from Sophos in 2023 indicated that 66% of healthcare organizations were hit by ransomware, with 34% experiencing data encryption and significant downtime. These attacks don't just compromise data; they jeopardize patient care. The 2020 ransomware attack on Düsseldorf University Hospital in Germany led to the first confirmed patient death linked to a cyberattack when care was delayed due to system outages.

Medical Devices Are a Weak Link

Modern hospitals rely heavily on Internet of Medical Things (IoMT) devices, ranging from insulin pumps to MRI machines. According to a study by Cynerio, 53% of connected medical devices have a known critical vulnerability, yet patching them is often delayed due to clinical downtime risks. These unprotected devices offer easy entry points for lateral attacks across hospital networks.

Insider Threats and Human Error Persist

Verizon's 2024 Data Breach Investigations Report found that 35% of healthcare breaches involved internal actors, often due to poor access controls or lack of cybersecurity awareness. Simple mistakes—like misaddressed emails or weak passwords—account for a significant portion of breaches, indicating a need for stronger policies and staff training.

Regulatory Pressure Is Increasing

Globally, regulators are tightening compliance demands. HIPAA in the U.S., GDPR in Europe, and DPDPA in India all impose strict requirements around data privacy and breach reporting. Non-compliance now leads to multi-million-dollar fines and reputational damage, amplifying the financial stakes for lax security.

A CALL TO ACTION

Healthcare security is no longer just an IT concern—it's a patient safety issue. Organizations must treat cybersecurity as a strategic priority, investing in threat detection, incident response, zero trust architectures, and regular employee training. The cost of inaction isn't just financial; it could mean lives lost and trust destroyed.

Security in healthcare is not just about protecting data. It's about protecting people.

Strengthen Cybersecurity Governance

Involve board into Cybersecurity and adopt industry standards and frameworks.

Protect Patient Data with Zero Trust Architecture

Implement stringent access control measures, encryption standards and network segmentation

Strengthen Defences Against Ransomware

Perform continuous threat monitoring, be ready with incident response plans and have Backups secured.

Secure Medical Devices (IoMT)

Maintain an up-to-date asset inventory, continuously discover and patch vulnerabilities, implement IoMT on separate VLANs with restricted access.

Build a Security-Aware Workforce

Carry out training and simulation exercises, identify security champions, and communicate established security policies.

Conduct Regular Assessments and Audits

Simulate attacks to discover exploitable vulnerabilities, ensure regular audits, and cover third parties for Risk assessments.

Healthcare organizations must move from reactive defence to proactive resilience. Cybersecurity should be embedded into the design of healthcare systems—not retrofitted after an attack. When done right, these efforts can protect not only data but also clinical outcomes, financial health, and public trust.