iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

STRENGTHENING THE RESILIENCE OF CRITICAL MEDICAL DEVICES AND IOT INFRASTRUCTURE AGAINST CYBER THREATS

Eniola Akinola Odedina
Covenant University

ABSTRACT
Given that the healthcare sector is steadily accepting Internet of Things (IoT) technologies and being connected with networked medical devices, the sector is becoming more vulnerable to very sophisticated cyber threats. These are devices ranging from insulin pumps and pacemakers to hospital-wide monitoring systems that are necessary to patient care and to an efficient operation. While this connectivity gives them functionality, they are also exposed to risks of ransomware attacks, data breaches, as well as life threatening manipulation. This article looks at the real threat landscape facing critical medical and IoT devices in a more broad sense and explores real world incidents and systematical vulnerabilities. It focuses on securing legacy systems, the design constraints involved in creating embedded device and regulatory gaps. A multi layered resilience framework that is based on cybersecurity-by design, zero trust architecture and AID driven threat detection is proposed. In addition, it examines how regulatory bodies, international coordination, and the moral obligation to put safety of patients first, serve to assist in achieving the objective. This work has the goal of being a roadmap for healthcare institutions, device manufacturers, and security professionals to work simultaneously to strengthen the digital backbone of today's medicine.

Keyword:
Cybersecurity, Medical devices, Lot infrastructure, Resilience, Healthcare technology

1. INTRODUCTION

Modern medical devices and the Internet of Things systems help healthcare organizations simultaneously provide better care and safer treatment. Medical technology, such as biosensors and artificial intelligence, enhances how healthcare works and manages health systems (Cheung et al., 2019; Chong, Blut, & Zheng, 2022). While innovative systems help hospitals advance technology, they are more vulnerable to cyber dangers.

1.1 The Growing Cybersecurity Threat in Healthcare: Healthcare facilities have become favorite targets of online criminals. Healthcare facilities remain at risk because delivering service remains important while their technology infrastructure stays old and weak. Medical IoT (MIoT) product risks are greater than those of other device types because of three critical factors that make them vulnerable to threats.Limited onboard security features, Poor firmware update mechanisms, and Multiple communication networks function differently from each other. Modern healthcare facilities face real threats to patient safety and medical operations from cyberattacks, including ransomware attacks, unauthorized breaches of medical data, and device modifications made by hackers (Fernandez De Arroyabe et al., 2023; Sarker et al., 2020).

1.2 Regulatory Responses and Current Gaps: The official bodies now require companies to take security precautions to address these concerns. The EU Medical Device Regulation (MDR) now requires enhanced cybersecurity features for medical devices, according to Beckers, Kwade, and Zanca (2021), as well as Niemiec (2022). However, gaps remain. Current clinical technologies did not build cybersecurity features at the design stage. Regular cybersecurity checks usually fail to match the fast-changing cyber threats and unpredictable security risks (Slapničar et al., 2022)

1.3 Motivation and Goals: Our study comes forward because healthcare facilities and IoT systems need stronger protection from digital security threats that are growing in complexity. This study uses a complete resilience concept that combines anticipation with effective handling and restoration after disruptions (Duchek, 2020; Folke et al., 2010).

Here are the primary objectives this text needs to achieve:

- Detect the problems in device and system technology and policymaking that reduce their resistance to threats.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- Develop a security and resilience solution framework for application across device design through operations.
- Describe how adaptive systems and organizational readiness produce secure operations and stable outcomes.

1.4 Methodology and Scope: The research uses conceptual and integrative methods to evaluate the existing literature on cybersecurity, policymaking, organizational resilience, and health technology. It draws on Cybersecurity experts Fernandez de Arroyabe and colleagues released facts about healthcare businesses and security measures in 2023, Insights into audit and compliance mechanisms (Slapničar et al., 2022), Our analysis uses machine learning systems to find security threats, according to Sarkeret al. (2020). And theoretical models of resilience (Duchek, 2020; Folke et al., 2010).

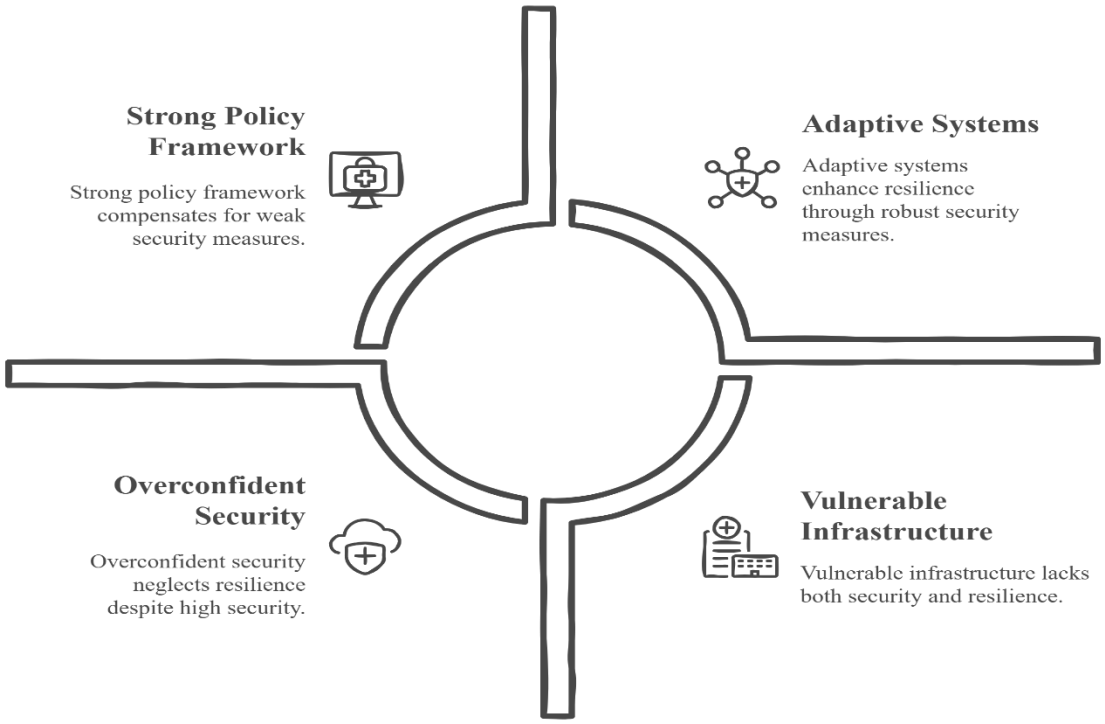

Figure 1: Cybersecurity Resilience in Healthcare

2. THE THREAT LANDSCAPE: CRITICAL RISKS AND EMERGING TRENDS

Healthcare organizations experience more security risks because digital transformation has made their systems easier to target. Medical Internet of Things devices face great danger due to their internet connections, essential medical operations, and weak security systems.

2.1 Common Attack Vectors on Medical Iot Devices

Cybercriminals seek to attack a Iot devices because they have three main weaknesses

- Medical Iot devices maintain complete functionality for long periods before update options arrive.
- Poor native security protection is a problem.
- Integration with sensitive clinical systems (Sarker et al., 2020).

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Medical computers usually send data across weak networks that hackers can breach. The manufacturer includes built-in login details for new devices, but users typically ignore replacing them. Old device firmware makes known security flaws easy to exploit. Poor RDP and Telnet settings enable unauthorized parties to enter hospital medical systems. According to Fernandez De Arroyabe et al. (2023) organizations poorly allocate security spending so their device weaknesses stay constant across healthcare system. Specific major incidents show us that our security systems stay weak inside

2.2 High-Profile Case Studies Demonstrating Systemic Vulnerabilities

2.2.1 WannaCry Ransomware and the NHS: The NHS faced severe service interruptions during the WannaCry ransomware attack 2017 because it had not updated its Microsoft systems. The disruption showed how unacceptable older computer programs remain in essential settings.

2.2.2 Insulin Pump Exploits: People found ways to control wireless insulin pumps from a distance. Security experts demonstrated how anyone with simple equipment could send harmful insulin levels or stop the proper dose timing. The weaknesses developed because data sent over networks lacked protection and needed added authentication systems.

2.2.3 Cardiac Device Recalls: In 2017 the FDA recalled half a million pacemakers because of their major security weakness. The security problems in medical devices let hackers turn settings or empty batteries at a distance, which puts patient lives at risk, so better hardware security must be developed.

2.3 Emerging Threats: Evolution in Cyber Offense Capabilities

2.3.1 Emerging Threats: Evolution in Cyber Offense Capabilities. Although security systems now defend more effectively, targets improve their attack techniques. Emerging threats now include:

2.3.2 AI-Powered Cyberattacks: Cybercrime evolves beyond malware because trained cybercriminals apply AI to generate attacks that escape regular firewalls and security devices. Their system updates tactics automatically to become harder to locate.

2.3.3 Firmware-Level Malware: This type of malware distinguishes itself from OS-level threats since it buries into the firmware, where it can remain even after the system resets. These threats become most dangerous in devices requiring long periods without software updates to stay functional.

2.4 Human Factors: The Persistent Weak Link

2.4.1 Supply Chain Vulnerabilities: Manufacturers and outsourcing parties more often introduce cyber threats as manufacturing and third-party sourcing progresses. The medical system may receive infected startup codes and defective parts from suppliers even before clinical use, according to Taherdoost (2022). These assaults are brutal to find and pose massive risks to systems. The Persistent Weak Link, Technology defenses help defend us, but human behavior remains the most significant security weakness.

2.4.2 Phishing and Social Engineering: Healthcare staff members become easy victims for phishing attacks since attackers send fake urgent updates that look official from IT and administrative teams. A single weak attack enables successful access violations plus malware distribution into systems.

2.4.3 Insider Threats: A person with permission to access system areas can break through any security defense regardless of its power. Network hackers break in through both intended data releases and unintended system setup errors. Weak Cyber Hygiene Practices users with poor security habits make system weaknesses when they repeat passwords, do not update their programs, and break protocol rules. Fast medical settings tend to give less weight to cybersecurity despite clinical requirements, putting these facilities at more risk. Slapničar and colleagues (2022) assert that cybersecurity audits should encompass human conduct in their evaluation since technical protections alone are ineffective without the proper user habits and security comprehension.

Summary of Threat Landscape

Healthcare and MIoT networks operate inside a diverse and progressively developing attack environment. Existing system weakness continuously overlaps with new risks, such as cyberattacks automated by AI and cyberattacks coming through supply chain partners. The weakest link of cybersecurity systems is often made up of their human users. A complete response must fix technological weaknesses and human behavior problems within medical facilities.

3. TECHNICAL VULNERABILITIES IN MEDICAL DEVICES AND IOT SYSTEMS

Healthcare providers have serious security problems because their linked technologies often have weak security in medical devices plus IoT systems. Medical IoT operates under very constrained conditions in specific settings,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

making establishing basic security measures hard. This section defines the main technical weaknesses that allow hackers to attack sensitive medical assets.

3.1. Legacy Systems and the Absence of Update Mechanisms

Hospitals use older medical devices because cybersecurity matters were not addressed during their design phase. These devices use outdated operating systems from Windows XP or self-made firmware that companies stopped providing security updates for. Newer medical devices created without OTAs make it nearly impossible to install essential software updates after setting them up. The consequences are significant: Vulnerabilities remain unpatched for years, The digital equipment does not work correctly with new security-focused network systems, Manual device updating creates both work slowdowns and puts patient safety at risk. Research by Fernandez De Arroyabe et al. in 2023 found that slower patch development made UK organizations frequently fail cybersecurity audits because they work with outdated tech.

3.2 Insecure Wireless Communication Protocols

Medical devices require wireless communication standards to make patients more mobile and easy to use. Bluetooth Wi-Fi Zigbee and proprietary RF signals appear together with wearable sensors, infusion pumps, and patient monitors. However, many of these devices: Transmit data without encryption, Failed to authenticate data sources. These medical devices use wireless networks that were made earlier or support weak security methods. The lack of protection against harmful network activities makes devices vulnerable to middleman security threats and unauthorized system-control actions. Toxic effects can involve significant private information theft and device manipulation to threaten human life, especially when targeting medical devices like pacemakers and insulin pumps. Sarker and colleagues showcased in their 2020 research how medical IoT systems experience security data transmission flaws while real-time requirements make encryption protocols harder to implement.

3.3 Limited Processing Power and Weak Encryption

The devices used in MIoT have basic processors that use little power and have little internal storage. These restrictions make it difficult for them to execute advanced cryptographic tasks such as instant encryption and decryption and secure key sharing.

This results in:

- The devices rely on poor encryption standards from earlier times.
- Avoidance of end-to-end encryption,
- Limited compatibility with secure communication frameworks such as TLS 1.3.

Research teams are creating simpler encryption methods, yet these new algorithms are limited in usage since companies wait for clear rules and standard protocols before implementing them. Modern devices' basic security functions to run smoothly create openings hackers can use to access them.

3.4 Hardcoded Credentials and Insecure APIs

Many devices enter the market with preprogrammed administrative access details that are permanent parts of the firmware. These credentials are often: Universal across devices, No changeable by users, IT personnel responsible for maintenance do not have correct documentation of internal users. When attackers break into a single device or firmware model, they immediately access all devices from the same product line. APIs enabling data sharing with external platforms come with basic security vulnerabilities, a common problem. Common API issues include:

- Lack of authentication or token validation
- Exposure of sensitive patient data in plain text
- Not setting limits for requests allows unauthorized users to knock systems offline.

According to Slapničar et al. (2022), their cybersecurity audits found that insecure credentials management and API failures consistently pose significant threats in medical device networks.

3.5 Device Interdependencies and Network Exposure

Medical facilities now link multiple monitoring devices to pumps and electronic health record systems by exchanging data directly in real-time. The ability of different medical devices to communicate makes protection harder to maintain. A device with compromised security becomes a gateway for unwelcome access into the entire network and defeats its security measures. Common risks include:

- Trust-based communication between devices with no mutual authentication,
- Our network has no distinct blocks, which allows attackers to spread easily across all system areas.
- The network access system for devices does not maintain proper protection standards.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Medical device and IoT network weaknesses result from larger system issues developed in design practices and because of expense limitations and inconsistent regulator regulations. Medical device networks remain vulnerable to attacks because they use outdated system designs and operate through weak encryption and damaged security setups building network resilience requires us to include security basics. Using these connections simultaneously, the WannaCry attackers infected medical facilities worldwide during their assault. Increased device connectivity requires us to modify our network security approach according to the research findings of Beckers, Kwade, and Zanca (2021).

Table 1: Technical Vulnerabilities in Medical IoT Devices

Vulnerability Type	Description	Risk Level	Suggested Mitigation
Legacy Systems	Outdated OS and lack of update mechanisms	High	Secure decommissioning, OTA updates, periodic vulnerability scans
Insecure Wireless Protocols	Weak encryption and lack of authentication in Bluetooth, Wi-Fi, Zigbee	High	Enforce secure protocols (e.g., TLS 1.3), validate sources, upgrade device communication
Limited Processing Power	Cannot support strong encryption algorithms	Medium	Use lightweight encryption schemes; prioritize privacy-by-design during development
Hardcoded Credentials	Embedded admin credentials shared across devices	High	Mandate unique credentials, implement credential rotation and secure storage
Insecure APIs	Lack of authentication, exposure of data in plain text	High	Use token validation, encrypt API traffic, limit request rates
Device Interdependencies	Networked devices allow lateral movement by attackers	High	Implement segmentation, device-level access control, mutual authentication

4. RESILIENCE STRATEGIES: TECHNICAL, INSTITUTIONAL, AND DESIGN PERSPECTIVES

Our healthcare systems must adopt complete protection methods to address the expanding use of IoT medical devices, which is vital now. Building organizational resilience means blocking cyber threats, preparing to spot destructive threats, and successfully handling any incidents that occur (Duchek 2020; Folke et al. 2010). This section explains the essential strategies needed to secure a solid healthcare system at technical, organizational, and device levels.

4.1 Cybersecurity-by-Design: Secure Development Life Cycles

Secure medical IoT systems start with cybersecurity-by-design, where designers build security at each step of the device life cycle, from development to retirement. Key principles include:

- Security analysis early in development helps find risks to protect the system before production begins.
- Our organization follows both secure development methods plus select proven software features.
- A complete security check using penetration testing and code review needs to happen before launching the devices.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

EU MDR and FDA now require medical device manufacturers to adopt secure development life cycles through their legitimate guidance documents (Beckers et al., 2021; Niemiec, 2022). Most outdated systems avoid reaching regulatory control, exposing them to security threats.

4.2 Zero Trust Architecture and Network Segmentation

The traditional perimeter security design works poorly with current heterogeneous mobile medical devices. Under Zero Trust Architecture (ZTA), systems assume nothing about trust, so everything entered requires regular proof and verification (Taherdoost, 2022).

In practical terms, ZTA includes:

- Our network design uses small sections to block attacks from spreading through different areas.
- A system checks access according to job duties plus authenticates user identities.
- Continuous monitoring of user behavior and device communication.

Under this security method, ZTA creates protective boundaries between critical hospital systems, including patient monitors, electronic health record storage, and infusion pumps, reducing the area affected by a security break.

4.3 AI/ML for Threat Detection and Predictive Analytics

Healthcare systems have grown large and complex; therefore, AI and machine learning play a major role in quickly detecting threats and predicting future security risks. The systems learn normal operations before identifying these problems; Unusual device communication patterns, Irregular firmware behaviors, Unauthorized data exfiltration attempts. Sarker et al. (2020) proved that machine learning systems work well to find new cyber threats and lower false detection numbers. The medical setting demands simple, explainable models that require excellent data quality and continuous training to succeed in this challenging field.

4.4 Our organization needs effective OTA and patch update systems.

Protecting medical devices calls for thorough patch updates to block recognized system weaknesses. Medical facilities must keep device systems running because they support patient treatment 24/7. Solutions include:

- Medical devices receive updates through a wireless network known as OTA updates without physical disruptions.
- Secure update technology lets medical staff contain device failures while maintaining safe patch implementations.
- Validation in controlled environments before wide-scale patch deployment.

Manufacturers need to put secure update systems in place to meet their legal requirements in monitoring medical devices after production (Beckers et al., 2021).

4.5 Organizational Preparedness: Cyber Incident Response Plans.

Technical defenses alone are insufficient. Healthcare organizations must develop unique cyber incident response procedures for their medical setting. These plans should include:

- Defined roles and responsibilities for clinical, IT, and executive teams.
- Decision-making protocols for containment, communication, and recovery.
- Integration with local emergency management and regulatory bodies.

A thoroughly planned CIRP reduces data loss and downtime and shields organizations from reputation and legal hazards after an incident (Duchek, 2020).

4.6. Workforce Training and Cybersecurity Simulations

Human error becomes a major target for cybercriminals in healthcare information security. An organization learns security practices better when it routinely executes training and simulation exercises. Our organization helps clinical and administrative staff recognize emails that can hurt our system. Each user group should learn about correct device usage, data protection rules, and incident reporting steps. Medical facilities practice real-life exercises to mimic attacks against their system, such as ransomware and data theft. These activities teach IT and clinical staff to simultaneously detect risks and follow safety procedures (Slapničar et al., 2022).

4.7 Third-Party Risk Management

Medical systems require collaboration with numerous external suppliers who provide cloud services EHR platforms and medical device units. Each external party poses safety weak points in this system. Healthcare organizations should take these specific actions to handle the security risks they face. Check third-party suppliers for security through evaluations and testing. Implement security standards as conditions for buying and working together with our partners and suppliers. Organizations should expect suppliers to share details about their security practices and public breaches. Neglecting third-party network security guidebooks brought about many major

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

healthcare data break-ins during recent years, causing us to realize the importance of proper risk management protocols (Fernandez De Arroyabe et al., 2023).

4.8 Case Examples of Effective Mitigation Strategies

4.8.1 Ransomware Resilience at a German Hospital (2021)

The university hospital in Düsseldorf successfully reduced ransomware attack damages through micro-segmentation of affected areas plus manual backup restoration before transferring non-emergency patients to partner hospitals. These flexible actions revealed that combining various backup systems works in emergencies to preserve human lives.

4.8.2 The Mayo Clinic set up a Zero Trust security system as their second example.

People in healthcare security see the Mayo Clinic as a model organization for implementing Zero Trust security in stages. The organization defends its systems by dividing its network into segments and enforcing controlled user access rules plus detailed activity records.

4.8.3 NHSX in the UK demonstrated their Resilience Strategy through their security plan

NHSX built a national cybersecurity program with rules that forced emergency reporting, plus an intelligence-sharing system for protecting infrastructure vendors. The initiative demonstrates how top-level leadership ensures good security practices across different parts of an organization.

4.9 Importance of Public-Private Collaboration

Every stakeholder needs partnerships to achieve resilience in cybersecurity. It helps organizations use knowledge and best practices to develop standard safety measures against new security risks. Key areas for collaboration include:

- The government and private sector develop security measures to produce workable technical safety requirements.
- Public funding for security R&D, especially in AI-driven risk detection.
- Information-sharing platforms like Information Sharing Analysis Centers let users access up-to-date threat data immediately.

Technical updates alone are not effective in creating resilient medical IoT networks. Real resilience for medical IoT needs combined efforts from experts to build security from the start, ongoing tracking of threats, getting systems ready, and sharing responsibilities across healthcare teams. These security strategies will keep healthcare digital development safe for patients and prevent system failures as medical technology grows more sophisticated**.** The EU Horizon Health initiative together with US Healthcare Sector Coordinating Council demonstrate how organizations use cross-sector partnerships to create stronger security systems for healthcare (Taherdoost, 2022; Niemiec, 2022).

5. CONCLUSION - FUTURE DIRECTIONS AND POLICY RECOMMENDATIONS

Digital healthcare needs new technologies and secure infrastructure to replace improper and temporary cybersecurity methods. This section outlines what needs to be achieved through new technology development plus effective decision-making to create a secure healthcare system for the future.

5.1 Innovations in Secure Medical Technologies

5.1.1 Blockchain for Identity and Data Management

Medical IoT networks handle data and identity securely because blockchain technology spreads trust and encryption across multiple computers. Healthcare providers can confirm device quality and monitor software updates while protecting system access through network-wide distributed ledgers, according to Taherdoost (2022). Adding blockchain to device communication channels helps stop unauthorized data changes as they happen.

5.1.2 Post-Quantum Encryption

Modern medical IoT devices have weak cryptographic protection since they cannot resist quantum computing's developing power. PQC is an advanced defense technology that shields against data threats because current encryption models will no longer work against future quantum threats. Research groups and standards experts should set PQC algorithms as the main technical choices when developing essential medical devices that need long-term support in critical care facilities.

5.2 Strengthening International Standards and Harmonization

The scattered system for controlling medical devices makes consistent cybersecurity protection difficult. Though the EU Medical Device Regulation (MDR) added cybersecurity components to their rules in 2021, Beckers et al. struggled between countries to create standard protection methods. Organizations should cooperate to create a

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

standard set of rules that fill all existing gaps in medical device regulation. Alignment of cybersecurity standards across jurisdictions (e.g., ISO/IEC 81001, NIST, IMDRF guidelines). The medical industry should establish a single organization to maintain security standards with updated technological information. Development of everyday language and threat taxonomies for medical IoT security. This approach helps authorities quickly evaluate products from different countries while informing consumers about supplier networks and responding faster to new security threats.

5.3 Mandatory Cybersecurity Certification for Devices

Guidelines that businesses follow by choice have not proved strong enough to guarantee security standards. Companies selling medical IoT products must pass cybersecurity tests as a regulatory requirement to safeguard basic protection standards, like health authorities or regional centers. Formal certification systems for cyber security need to follow the same approach as described by Slapničar et al. in 2022. Validation of software integrity and secure boot processes, Penetration testing and vulnerability assessments. The process needs security documentation from the development process to the decommissioning process. Manufacturers must prove their efforts, while healthcare providers could better trust device security controls with these new standards.

5.4 Building Resilience into the Device Lifecycle

Companies should design cybersecurity across all phases of their devices to better protect healthcare systems. To enhance cyber defense, devices must anticipate problems and react to interruptions according to resilience principles (Duchek 2020 and Folke et al. 2010). This requires:

- Secure-by-design and privacy-by-design principles during development.
- The system integrates AI technology to detect events outside usual operation standards (Sarker et al., 2020).
- Devices automatically receive updates through the air to prevent clinical interruptions.
- End-of-life protocols for secure decommissioning of obsolete devices.

Including resilience elements in each production and retirement phase helps medical systems adapt better to unknown situations.

5.5 Strategic Policy Proposals: A Call to Action

A collective effort from different groups will help put these recommendations into action. All major players in healthcare systems and technology manufacturers worldwide should work together to build a strong threat-preventing medical technology system. Policy directions include; Governments should enforce new rules regarding healthcare technology safety assessments, such as how environmental impacts need testing, Private sector companies and public organizations should work together to develop and test secure technologies through combined investment and shared development projects, Companies that build advanced security by implementing PQC and blockchain technology would receive priority evaluation from regulators, plus tax credits, Healthcare needs CSIRT teams to handle security incidents for local response and national defense.

Table 2: Strategic Policy Recommendations and Responsible Stakeholders

Recommendation	Responsible Entity	Timeline
Enforce cybersecurity certification for medical IoT devices	National regulators (e.g., FDA, EMA)	Short–Mid Term
Mandate post-quantum encryption and blockchain integration	Device manufacturers, standards bodies	Mid–Long Term

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Align global cybersecurity standards (ISO, NIST, IMDRF)	International regulatory consortia	Mid Term
Establish national CSIRT teams for healthcare	Government agencies, health ministries	Short Term
Incentivize secure tech adoption via tax credits	National governments, policy makers	Mid Term
Fund R&D in AI-driven threat detection	Public-private partnerships, innovation hubs	Ongoing
Require resilience throughout device lifecycle	Manufacturers, accreditation bodies	Short–Mid Term

5.6 Final Reflections on the Future of Secure, Resilient Healthcare Infrastructure

The medical industry needs to develop digital systems at the same security level as its future advancements. According to Fernandez De Arroyabe et al., 2023 higher cybersecurity investments result in more cyberattacks against organizations despite raising employees' cyber awareness. Healthcare facilities should change their approach from blocking attacks to preparing against future threats. This vision includes:

- The security framework develops in sync with growing threats in the environment.
- Our company focuses on creating strong trust, protection, and the ability to recover when needed.
- A worldwide group of people unite to safeguard the digital support structure of medical treatment.

Over the next years healthcare organizations will have to achieve basic security and resilience standards for patients to trust their care while systems stay active and patients stay safe.

REFERENCES

1. Alqudah, A. A., Al-Emran, M., & Shaalan, K. (2021, November 1). Technology acceptance in healthcare: A systematic review. Applied Sciences (Switzerland). MDPI. https://doi.org/10.3390/app112210537
2. Bach, P. M., Deletic, A., Urich, C., Sitzenfrei, R., Kleidorfer, M., Rauch, W., & McCarthy, D. T. (2013). Modelling Interactions between Lot-Scale Decentralised Water Infrastructure and Urban Form - a Case Study on Infiltration Systems. Water Resources Management, 27(14), 4845–4863. https://doi.org/10.1007/s11269-013-0442-9
3. Beckers, R., Kwade, Z., & Zanca, F. (2021). The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics. Physica Medica, 83, 1–8. https://doi.org/10.1016/j.ejmp.2021.02.011
4. Chau, K. Y., Lam, M. H. S., Cheung, M. L., Tso, E. K. H., Flint, S. W., Broom, D. R., … Lee, K. Y. (2019). Smart technology for healthcare: Exploring the antecedents of adoption intention of healthcare wearable technology. Health Psychology Research, 7(1). https://doi.org/10.4081/hpr.2019.8099
5. Cheung, M. L., Chau, K. Y., Sum Lam, M. H., Tse, G., Ho, K. Y., Flint, S. W., … Lee, K. Y. (2019). Examining consumers' adoption of wearable healthcare technology: The role of health attributes. International Journal of Environmental Research and Public Health, 16(13). https://doi.org/10.3390/ijerph16132257

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

6. Chong, A. Y. L., Blut, M., & Zheng, S. (2022). Factors influencing the acceptance of healthcare information technologies: A meta-analysis. Information and Management, 59(3). https://doi.org/10.1016/j.im.2022.103604
7. Connor, K. M., & Davidson, J. R. T. (2003). Development of a new Resilience scale: The Connor-Davidson Resilience scale (CD-RISC). Depression and Anxiety, 18(2), 76–82. https://doi.org/10.1002/da.10113
8. De Maria, C., Di Pietro, L., Díaz Lantada, A., Madete, J., Makobore, P. N., Mridha, M., … Ahluwalia, A. (2018). Safe innovation: On medical device legislation in Europe and Africa. Health Policy and Technology, 7(2), 156–165. https://doi.org/10.1016/j.hlpt.2018.01.012
9. Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. Business Research, 13(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7
10. Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers and Security, 124. https://doi.org/10.1016/j.cose.2022.102954
11. Festas, A. J., Ramos, A., & Davim, J. P. (2020, January 1). Medical devices biomaterials – A review. Proceedings of the Institution of Mechanical Engineers, Part L: Journal of Materials: Design and Applications. SAGE Publications Ltd. https://doi.org/10.1177/1464420719882458
12. Folke, C. (2016). Resilience (Republished). Ecology and Society, 21(4). https://doi.org/10.5751/ES-09088-210444
13. Folke, C., Carpenter, S. R., Walker, B., Scheffer, M., Chapin, T., & Rockström, J. (2010). Resilience thinking: Integrating resilience, adaptability and transformability. Ecology and Society, 15(4). https://doi.org/10.5751/ES-03610-150420
14. Herrman, H., Stewart, D. E., Diaz-Granados, N., Berger, E. L., Jackson, B., & Yuen, T. (2011). What is resilience? Canadian Journal of Psychiatry. Canadian Psychiatric Association. https://doi.org/10.1177/070674371105600504
15. Jarden, K. M., Jefferson, A. J., & Grieser, J. M. (2016). Assessing the effects of catchment-scale urban green infrastructure retrofits on hydrograph characteristics. Hydrological Processes, 30(10), 1536–1550. https://doi.org/10.1002/hyp.10736
16. Keutzer, L., & Simonsson, U. S. H. (2020, June 1). Medical device apps: An introduction to regulatory affairs for developers. JMIR MHealth and UHealth. JMIR Publications Inc. https://doi.org/10.2196/17567
17. Kumar, H., Singh, M. K., Gupta, M. P., & Madaan, J. (2020). Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework. Technological Forecasting and Social Change, 153. https://doi.org/10.1016/j.techfore.2018.04.024
18. Mohamed, R. (2009). Why do residential developers prefer large exurban lots? Infrastructure costs and exurban development. Environment and Planning B: Planning and Design, 36(1), 12–29. https://doi.org/10.1068/b33120
19. Niemiec, E. (2022). Will the EU Medical Device Regulation help to improve the safety and performance of medical AI devices? Digital Health, 8. https://doi.org/10.1177/20552076221089079
20. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021, December 1). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction. Elsevier B.V. https://doi.org/10.1016/j.ijcci.2021.100343
21. Rahman, M. S., Ko, M., Warren, J., & Carpenter, D. (2016). Healthcare Technology Self-Efficacy (HTSE) and its influence on individual attitude: An empirical study. Computers in Human Behavior, 58, 12–24. https://doi.org/10.1016/j.chb.2015.12.016
22. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00318-5
23. Shuster, W. D., Dadio, S., Drohan, P., Losco, R., & Shaffer, J. (2014). Residential demolition and its impact on vacant lot hydrology: Implications for the management of stormwater and sewer system overflows. Landscape and Urban Planning, 125, 48–56. https://doi.org/10.1016/j.landurbplan.2014.02.003

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

24. Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44. https://doi.org/10.1016/j.accinf.2021.100548
25. Taherdoost, H. (2022, July 1). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics (Switzerland). MDPI. https://doi.org/10.3390/electronics11142181