White Paper Executive Summary

Wanyi Fu (wqf5108@psu.edu) *Nish Barot* (tbb5439@psu.edu)

Project: Cybersecurity Protection of Humanoid Robots

Main Objectives:

1. Raise Public Awareness: Highlight the vulnerabilities of humanoid robots through accessible reports, media engagement, and real-world case studies.
2. Strengthen Engineer Accountability: Promote cybersecurity best practices in robotics development, emphasizing secure coding, encryption, and threat modeling.
3. Provide Policy Guidance: Deliver fact-based insights to lawmakers, identifying critical gaps in current standards and recommending safeguards.

Part I Vulnerabilities of Humanoid Robots Cybersecurity

A robot is any automatically operated machine designed to replace human effort, regardless of whether it resembles a human in appearance or performs tasks in a human-like manner. The recent digital revolution promotes robots to become integrated more than ever into our life, which are devoted to serve, facilitate, and enhance the human life. Humanoid robots are designed to mimic human form and functions. In general, humanoid robots have a torso, a head, two arms, and two legs, though some humanoid robots may replicate only part of the body. They are widely used in sectors like defense, education, and hospitality, where they show great potentials to improve our life.

Despite the benefits of robotics, significant security concerns remain, posing risks to both humans and machines, one of which is from cyberattacks. Cyberattacks on robots involve threats like malware, data breaches, and system manipulation, aiming to compromise robotic devices, their software, or the data they process. These attacks can disrupt robot functions, steal sensitive information, or even cause physical harm, highlighting the need for strong cybersecurity measures in robotic systems.

Unintended accidents will always take place, but the ones caused by malicious attacks represent a very challenging issue. This includes maliciously hijacking and controlling robots and causing serious economic and physical losses. In October 2016, the “Mirai” malware infected numerous IoT devices, such as cameras and routers, forming a botnet that launched a large-scale distributed denial-of-service (DDoS) attack on the DNS service provider Dyn, which disrupted access to major websites like Twitter and Netflix, highlighting the significant cyber risks posed by IoT devices. Industrial robots are vulnerable to manipulation, and in 2019, cybercriminals extorted $6.9 million from manufacturing facilities. Notable companies such as Honda and Aebi Schmidt also suffered production stoppages due to such attacks. In 2021, an engineer was reportedly attacked by a robot at the Giga Texas factory near Austin, resulting in injuries and bloodshed. The cause of the incident has not been disclosed, however, the attack raises concerns over Cybersecurity.

Cybersecurity refers to technologies, practices and policies for preventing cyberattacks or mitigating their impact, which aims to protect networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Researches underscore significant cybersecurity vulnerabilities in robotic systems, revealing that even individuals without prior knowledge of robotics can potentially breach humanoid robots and their environments. However, it also highlights the contextual nature of such attacks - no universal penetration method exists, and attackers must rely on social intelligence to tailor strategies accordingly. Thus future studies could examine deeper into robotics security vulnerabilities, increase our understanding of cybersecurity measures, and inform the design of more resilient security

mechanisms.

Reference

[1] *What is Cybersecurity*, https://www.cisa.gov/news-events/news/what-cybersecurity (last visited Apr. 22, 2025)

[2] Yaacoub, JP.A., Noura, H.N., Salman, O. et al. *Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations.* Int. J. Inf. Secur. 21, 115–158 (2022). https://doi.org/10.1007/s10207-021-00545-8

[3] Patel, Y., Rughani, P.H. (2024). *Unmasking the Vulnerabilities: A Deep Dive into the Security Threat Landscape of Humanoid Robots.* In: Singh, Y., Singh, P.K., Gonçalves, P.J.S., Kar, A.K. (eds) Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2023. Lecture Notes in Electrical Engineering, vol 1194. Springer, Singapore. https://doi.org/10.1007/978-981-97-2839-8_19

[4] Alessio Botta, Sayna Rotbei, Stefania Zinno, Giorgio Ventre, *Cyber security of robots: A comprehensive survey*, Intelligent Systems with Applications, Volume 18, 2023, 200237, ISSN 2667-3053, https://doi.org/10.1016/j.iswa.2023.200237.

[5] Mirai (malware), https://en.wikipedia.org/wiki/Mirai_(malware). (last visited Apr. 22, 2025)

[6] Hongyi Pu, Liang He, Peng Cheng, Jiming Chen, Youxian Sun, *CORMAND2: A Deception Attack Against Industrial Robots*, Engineering, Volume 32, 2024, Pages 186-201, ISSN 2095-8099, https://doi.org/10.1016/j.eng.2023.01.013.

[7] Naveen Goud, Tesla AI Robot Attacks raises concerns over Cybersecurity, https://www.cybersecurity-insiders.com/tesla-ai-robot-attacks-raises-concerns-over-cybersecurity/, (last visited Apr. 22, 2025)

Part II Summary of Expert Advice

1. Dhananjai Senthil Kumar (technical expert)

Introduction: Dhananjai Senthil Kumar is a senior Computer Science student at Northeastern University and the founder of Rev. He has a background in robotics starting from high school (FIRST Robotics Challenge) and continuing into college research and projects, accumulating roughly 5 years of intermittent experience. He is currently working on developing a "Locobot", essentially a Roomba base with an arm and sensors (camera, Lidar), intended to function as a robotic waitress in restaurants.

Summary of interview:

Dhananjai Senthil Kumar gave us his opinions on robotics development and security considerations. He is currently developing a "Locobot"—a modified Roomba base equipped with an arm and sensors (camera, Lidar) designed to function as a robotic waitress in restaurants. The project, still in the R&D phase, focuses on environmental mapping, path planning, human interaction, and object manipulation (e.g., picking up dishes). While functionality is the primary focus, Dhananjai has implemented basic security measures: data is processed locally (onboard or on-premise), serialized rather than stored as raw images, and accessed via secured local networks with SSH and potential two-factor authentication (2FA). However, advanced cybersecurity hardening, such as encryption or automated updates, remains a future goal.

Security challenges are acknowledged but not yet prioritized. The system relies on Linux user permissions and physical oversight by restaurant owners to mitigate tampering risks. A kill switch and fail-safe protocols ensure the robot stops safely during failures or network drops. Dhananjai admits vulnerabilities exist, particularly in physical tampering or sensor manipulation, but believes current measures suffice for the R&D stage. Future plans include a mobile app for monitoring and updates, alongside potential AI-driven adaptations inspired by autonomous vehicles and GDPR principles (e.g., data minimization).

Liability for security breaches is seen as shared between developers (for software flaws) and users (for network/physical security). While terms and conditions are planned, specific legal protections for consumers remain undefined. Dhananjai advocates for government regulations prioritizing physical safety standards (e.g., reliability metrics like "five nines") and data privacy, though he notes cybersecurity is secondary in his current phase.

The interview highlights a pragmatic, iterative approach to robotics development, where functionality precedes advanced security. Dhananjai's project reflects broader trends in emergent robotics: balancing innovation with nascent safeguards, while looking to industries like IoT and autonomous vehicles for future best practices. His focus on local data processing and modular upgrades underscores a cautious but forward-looking stance, aiming to eventually align with regulatory and consumer expectations as the technology matures.

2. Rudan Cheng (academic expert)

Introduction: Professor Rudan Chen, Doctor of Law from Peking University (jointly trained at the Max Planck Institute for Comparative Public Law and International Law, Germany), is an Associate Professor and Master's Supervisor at the School of International Law, China University of Political Science and Law. Her academic focus was primarily on international trade and law & economics. In recent years, she begins to pay attention to law & technology and AI regulations.

Summary of interview:

Professor Chen draws critical parallels with existing IoT and smart home vulnerabilities while

examining technical challenges, regulatory shortcomings, and future mitigation strategies. Humanoid robots face three primary security threats: data security risks where sensors collecting visual, tactile, and voice data are vulnerable to interception or tampering during transmission and storage; control system vulnerabilities where AI decision-making algorithms could be maliciously manipulated; and privacy breaches in human-robot interaction through voice command hijacking or biometric data theft. While current technical solutions include real-time monitoring systems and blockchain-secured communication protocols, significant gaps remain in penetration testing and long-term reliability assessments, with core technologies like high-precision positioning still under development.

Professor Chen mentions a critical lack of unified security standards across the industry, with varying hardware interfaces and communication protocols among manufacturers complicating security synergies. China's MIIT has introduced 2023 guidelines to establish a safer industrial chain, but specific technical standards remain incomplete. Globally, regulatory frameworks lag behind technological advancements, with no dedicated robot safety laws currently existing - oversight relies instead on patchwork applications of IoT and AI regulations like EU AI Act and the GDPR. Additional complexities emerge from unresolved ethical and liability questions regarding accountability for autonomous robot decisions. Key systemic barriers include cost-safety tradeoffs that incentivize security compromises, insufficient interdisciplinary collaboration between relevant sectors, and a shortage of specialized professionals like “robot security engineers.”

To address these challenges, Professor Chen proposes a multi-pronged approach focusing on technological, standardization, regulatory and ecosystem improvements. This includes developing hardware-level security solutions like trusted execution environments, establishing industry-wide security certifications through organizations like the China Academy of Information and Communications Technology, enacting clear liability laws distinguishing manufacturer and user responsibilities, and fostering cross-industry collaboration through training programs. The report concludes that achieving secure human-robot coexistence demands synchronized progress across technology innovation, standardized governance, and international regulatory cooperation - a challenge as complex as the robots themselves, requiring coordinated efforts from manufacturers, policymakers and security experts to build a trustworthy human-robot ecosystem.

3. Brendan Bernicker (private sector legal expert & consumer protection expert)

Introduction: Brendan Bernicker is now a Visiting Assistant Professor at Penn State Law, and holds J.D. degree from Yale. One domain of his research focuses on AI law. Prior to joining the law faculty, Professor Bernicker has been working as legal practioner for private sector. With a mixing backgroud with programming skills, he has rich experience advising startups and small businesses on a range of matters, including data privacy compliance, litigation related to technology law and even AI system development.

Summary of interview:

With the rapid advancement of security technologies and the maturation of the cybersecurity industry, the increasing availability of skilled professionals has led to a gradual reduction in corporate compliance costs related to security measures. Compliance costs are decreasing, and risk of being sued is increasing, thus companies tend to comply in advance to avoid risks. In addition, to safeguard their commercial interests, enterprises strategically adopt cybersecurity protocols to mitigate data leakage risks and sustain a competitive advantage in data protection.

If a robot causes data leakage due to a hacker attack, responsibility will generally be allocated to the manufacturer and operator side instead of consumers. Under the joint liability regime of tort law, the specific determination should be based on the specific case, involving the manufacturer, operator, or user. Cross-border data flows face legal conflicts (such as China’s data localisation vs. EU

cross-border compliance), and companies usually resolve supply chain issues through contract negotiations.

If a robot causes physical harm due to product quality issues, product liability - strict liability applies, but psychological harm and emotional compensation are generally not covered by compensation. Data loss may be claimable, but businesses often use disclaimers to avoid liability. Consumers often overlook cybersecurity risks, and laws must ensure contract terms are fair (e.g., standard contract templates). Business bankruptcy may result in robots being unable to receive maintenance, harming consumer rights, but legal intervention in such market risks is limited.

Companies need to balance cybersecurity measures with user experience, as excessive protection may reduce product usability. Disclaimers and data ownership clauses tend to favour commercial interests but must avoid harming consumer rights. The EU's GDPR and AI Act have been criticised for being enacted too early and imposing high compliance costs. In contrast, the US's ‘wait-and-see’ regulatory approach is considered more flexible and pragmatic.

Consumers generally underestimate cybersecurity risks (e.g., dark web data breaches), while governments and businesses may exploit vulnerabilities for profit. Technical solutions must adapt to multi-jurisdictional legal requirements (e.g., data encryption, localization). It is recommend that regulations be dynamically adjusted to align with technological advancements, avoiding premature codification, and promoting collaboration between technology and law to lower compliance barriers for businesses.

4. Mingrui Fu (consumer)

Introduction: Dr. Mingrui Fu currently resides in Beijing, China, and holds a Ph.D. from Beijing University of Technology. Based on extensive experience using smart home devices (such as smart surveillance cameras, robotic vacuum cleaners, automatic pet feeders, smart speakers, and smart hubs, smart locks, thermostats), this individual was interviewed as a consumer with deep personal insights into the topic.

Summary of interview:

Dr. Fu, as a smart home enthusiast, primarily considers how devices can enhance convenience when making purchases. During actual usage, he gradually becomes aware of potential cybersecurity risks—for instance, after installing a smart camera, he pays close attention to reports about privacy breaches involving such devices. While using smart control panels and door locks, he also harbors concerns about network security, though he has never experienced any tangible losses. He believes these risks remain manageable and do not warrant excessive anxiety.

Regarding China's rapidly advancing humanoid robot industry, Dr. Fu maintains cautious optimism. He recognizes the potential of such products in eldercare, medical assistance, and household chores but is particularly concerned about cybersecurity. He argues that manufacturers should implement physical defense mechanisms alongside software protections to fully eliminate security vulnerabilities. As a consumer, he is willing to pay a premium for more secure models but prefers to wait until the technology matures before purchasing. Meanwhile he also advocates for better consumer education - raising awareness about cybersecurity risks while providing practical guidance on risk mitigation.

Dr. Fu emphasizes that, given the technical complexity of humanoid robots, regulatory bodies should enforce stricter oversight. However, he also expressed concerns about policymakers. He worries that due to insufficient understanding of the technology, current laws and regulations may fail to adequately address practical needs, resulting in regulatory loopholes or inadequate oversight. This "technology-policy" knowledge gap could undermine the effectiveness of regulatory systems,

exposing emerging technologies to risks of delayed or misaligned regulation.

5. Desirae Satterlee (consumer)

Introduction: Desirae Satterlee is a J.D candidate at Penn State Law, who lives in State College Pennsylvania. As a tech-savvy consumer, she owns an Ionvac robot vacuum and other smart home devices. While comfortable with basic data collection for product functionality, she has concerns about Wi-Fi-related data privacy and potential misuse.

Summary of interview:

Desirae Satterlee, a consumer with no formal robotics background, uses an Ionvac robot vacuum alongside other smart home devices. She chose the product primarily based on price and availability at a trusted retailer like Walmart. While comfortable with basic data collection (e.g., apartment layout and cleaning habits) for product improvement, she expresses concern about potential Wi-Fi data misuse, especially after reflecting on security vulnerabilities in other robotic devices.

Desirae admits she didn't read the terms and conditions during setup and was unaware of the specifics of data collection until prompted. She believes manufacturers and developers, not consumers, should bear responsibility for security flaws, as these devices are marketed as user-friendly. Though her current vacuum has no cameras and poses minimal perceived risk, she acknowledges that transparency, regular security updates, and third-party verification would be more critical for advanced robots (e.g., those with cameras or butler functions).

The conversation heightened her awareness of cybersecurity, prompting her to consider researching security reputations of brands before future purchases. While price and convenience remain her top priorities, she now sees value in independent certifications to ensure safer consumer choices. Her stance reflects a common consumer trend: balancing practicality with growing, albeit reactive, concerns about data privacy and device security.

6. Engagement with CPSC on Humanoid Robot Cybersecurity Concerns (consumer protection expert)

Our team attempted to contact the United States Consumer Product Safety Commission (CPSC) in writing to request a discussion with their experts regarding cybersecurity risks in humanoid robots. Unfortunately, we received no response. Upon reviewing their website and public records, we observed that CPSC's primary focus revolves around addressing physical harm and injuries caused by consumer products - particularly traditional hazards such as burns, fires, explosions, choking risks, and lead paint violations.

A search for "robot" on CPSC's website yielded only seven results, all related to physical safety issues: (1) Pool-cleaning robots recalled due to burn and fire risks (Aiper Elite Pro/Seagull Pro, 2023–2025); (2) Toy robots recalled for choking hazards (FAO Schwarz, 2022) or lead paint violations (OKK Trading, 2008; Schylling Associates, 2007); (3) Magnetic action figures (MagnaMan, 2008) and vintage toys (Voltron Lion, 1986) posing ingestion hazards.

These cases underscore CPSC's mandate: post-incident mitigation of tangible safety risks, rather than preemptive cybersecurity protections. While the Commission plays a critical role in addressing physical dangers, its framework appears ill-suited to regulate emerging threats like data breaches, unauthorized robot control, or AI-driven privacy violations in humanoid robot - unless such vulnerabilities directly cause bodily harm.

CPSC's reactive model prioritizes recalls and warnings after harm occurs, which is inherently inadequate for mitigating digital risks that require proactive safeguards (e.g., encryption, access controls). Given the absence of high-tech product oversight in their historical data, we conclude that

CPSC is unlikely to be a meaningful ally in advancing preventive cybersecurity standards for humanoid robots unless: A clear link between cyber vulnerabilities and physical injuries is established; or CPSC expands their scope of responsibility to cover digital consumer protections. For now, stakeholders may need to seek alternative regulatory pathways (e.g., FTC for data privacy, NIST for standards) to address these gaps.

Part III Summary of Key Elements for the Project to Succeed

1. Pre-Project Preparation and Comprehensive Planning

Objective: Lay a robust foundation to avoid oversights and unrealistic expectations.

Knowledge & Expertise:

- Conduct thorough research or consult experts to fill knowledge gaps.
  - Technical experts
    - Robotics engineers: Design safety and reliability (e.g., prevention of mechanical injury and system failure).
    - Cybersecurity experts: Prevent hacking and data leaks (e.g., privacy protection for home service robots).
  - Legal and compliance experts
    - Academic legal experts: Provide a macro framework (e.g., whether robots should bear legal responsibility, how the regulative framework should be built).
    - Practitioner Lawyers: Resolving specific issues (e.g., user agreement terms, product liability insurance).
  - User and Social Representatives
    - Consumer Protection Experts: Assessing product terms for potential rights violations (e.g., data ownership, disclaimer).
    - Real User Representatives: Testing usability through focus groups and collecting potential concerns (e.g., impact of security reputations on consumer behavior).
- Avoid assumptions; validate all critical aspects

Team & Collaboration: Assemble a multidisciplinary team with clear roles. Foster open communication to challenge biases and brainstorm risks.

Risk Assessment & Long-Term Vision: Identify direct and indirect consequences. Use scenario planning to anticipate "what-if" situations.

Cost-Benefit Analysis: Evaluate long-term costs beyond immediate expenses.

2. Implementation: Adaptability and Correction

Objective: Monitor progress and pivot as needed to mitigate unforeseen issues.

Iterative Testing: Pilot small-scale tests to evaluate outcomes, make use of new regulatory tools such as sandbox.

Real-Time Monitoring: Assign teams to track metrics and flag deviations (e.g., unexpected public backlash).

Flexible Decision-Making: Empower teams to halt or adjust plans if risks escalate (e.g., halt the project if safety is compromised).

3. Post-Project Review and Sustained Follow-Up

Objective: Ensure resolution of lingering effects and extract lessons.

Impact Assessment: Audit short- and long-term outcomes (e.g., social impact, community trust).

Accountability & Documentation: Debrief with stakeholders to document failures/successes. Update protocols to prevent repeat mistakes (e.g., stricter safety checks).

Ongoing Mitigation: Address latent issues.

Part IV Summary of Legal Analysis and Policy Concerns

1. Legal Challenges and Liability Frameworks

- Data Privacy & Protection
  - Humanoid robots collect sensitive biometric and behavioral data, raising concerns under laws like GDPR and China's Personal Information Protection Law (PIPL).
  - Ambiguities exist in data ownership, storage localization (e.g., China's data sovereignty laws vs. EU's cross-border flows), and user consent mechanisms.
- Liability for Breaches
  - Manufacturers/Operators typically bear responsibility for hacking-induced data leaks or physical harm under product liability laws (strict liability for defects).
  - Shared liability models may apply if user negligence (e.g., weak network security, choice to weaker security protection) contributes to breaches.
  - Psychological harm or emotional damages are rarely compensable, unlike physical injuries or data loss.
- Contractual Gaps:
  - Overreliance on disclaimers in user agreements risks unfair terms; standardized contracts are proposed to balance consumer rights and business interests.

2. Regulatory Gaps and Standardization Issues

- Fragmented Governance
  - No dedicated laws for humanoid robots; reliance on patchwork regulations (e.g., IoT safety standards, EU AI Act, GDPR).
  - China's 2023 MIIT guidelines aim to prompt the balance between development and security of humanoid robot but lack legal and technical specifics.
- Cross-Border Conflicts
  - Divergent security requirements complicate global deployments.
- Lack of Harmonized Standards
  - Varying hardware/software protocols across manufacturers hinder interoperability and security synergies.

3. Policy Recommendations

- Proactive Regulation
  - Dynamic laws: Avoid premature, rigid frameworks (e.g., critique of GDPR's high compliance burden); adopt iterative, technology-neutral rules.
  - Sector-specific standards: Mandate certifications (e.g., hardware-level encryption, penetration testing) via bodies like China Academy of Information and Communications Technology (CAICT).
- Stakeholder Collaboration
  - Public-private partnerships: Foster interdisciplinary cooperation among technologists, lawyers, and policymakers.
  - Consumer empowerment: Require transparency (e.g., clear data use policies) and third-party security audits.

- Institutional Reforms
  - Expand CPSC/FTC mandates to cover cyber-physical risks (beyond traditional injury-focused models).
  - Introduce “robot security engineer” roles to bridge technical-legal gaps.

4. Emerging Ethical and Enforcement Dilemmas

- Autonomy vs. Control
  - Unclear accountability for AI-driven decisions (e.g., if a robot’s manipulated algorithm causes harm).
- Cost-Safety Tradeoffs
  - Companies may deprioritize cybersecurity to cut costs or enhance usability, necessitating regulatory incentives.
- Global Coordination
  - Need for international treaties to address jurisdictional conflicts (e.g., U.S.-EU-China data flow disputes).

Conclusion

The legal and policy landscape for humanoid robot cybersecurity remains underdeveloped, with critical gaps in liability allocation, cross-border compliance, and standardization. A balanced approach - combining adaptable regulations, industry-wide certifications, and consumer-centric safeguards- is vital to mitigate risks while fostering innovation. Policymakers must act collaboratively to preempt threats without stifling technological progress.

Part V Concrete proposal for deployment with budget

To address cybersecurity protection for humanoid robots, a multi-faceted approach is necessary, encompassing corporate responsibility, regulatory frameworks, and consumer safeguards.

Below is a concrete proposal with budget estimates for each aspect:

1. Corporate Cybersecurity Measures for Humanoid Robots

Companies developing humanoid robots must prioritize embedded security protocols and proactive threat mitigation. Key initiatives include:

- **Technical Safeguards**
  - End-to-End Encryption & Secure Communication: Implement TLS 1.3 for data transmission and storage, with estimated costs of $500,000–$1M for development and integration[1][5].
  - Firmware Integrity Checks: Use code signing and blockchain-based verification systems to prevent unauthorized modifications. Budget: $300,000–$600,000 annually[1][4].
  - AI Model Hardening: Invest in adversarial training and real-time monitoring tools to detect manipulation. Cost: $1.2M–$2.5M for R&D and deployment[1][7].
  - Zero-Trust Architecture: Enforce multi-factor authentication (MFA) and least-privilege access controls. Budget: $200,000–$400,000 for implementation[1][5].
- **Operational Investments**
  - Cybersecurity Workforce: Hire 10–15 specialists (e.g., penetration testers, AI security experts) at $2M–$3.5M annually[3][5].
  - Third-Party Audits: Conduct biannual vulnerability assessments and penetration testing. Cost: $150,000–$300,000 per audit[2][4].

2. Regulatory System Development

Governments and regulatory bodies must establish enforceable standards to ensure accountability and interoperability.

- **Policy Frameworks**
  - Risk-Based Certification: Develop tiers for robot applications (e.g., high-risk medical robots vs. low-risk domestic assistants), modeled after the EU AI Act. Initial setup cost: $5M–$10M[4][7].
  - Lifetime Cybersecurity Requirements: Mandate over-the-air (OTA) updates and vulnerability disclosure processes. Budget for regulatory tech: $2M–$4M[4][7].
  - Global Harmonization: Fund international working groups to align standards (e.g., ISO/IEC 15408 for robotics). Annual cost: $1M–$2M[4][7].
- **Enforcement Mechanisms**
  - Compliance Audits: Allocate $3M–$6M annually for regulatory bodies to inspect manufacturers and levy fines for non-compliance[4][5].
  - Public Cybersecurity Database: Create a platform for reporting breaches and sharing threat intelligence. Development cost: $1.5M–$3M[6][7].

3. Consumer Protection Enhancements

Strengthening user rights and transparency is critical to building trust.

- **User-Centric Protections**

- Transparency Requirements: Mandate clear labeling of data collection practices and AI decision-making processes. Implementation cost: $800,000–$1.6M[5][6].
- Incident Response Funds: Establish a compensation pool for consumers affected by breaches. Initial funding: $2M–$5M[5][6].
- Education Campaigns: Launch public workshops and digital resources on robot safety. Annual budget: $500,000–$1M[6][7].

Legal Safeguards

- Strict Liability for Manufacturers: Align with the EU's revised Product Liability Directive, requiring companies to prove defect-free systems. Legal framework cost: $1M–$2M[4][6].
- Biometric Data Protections: Enforce state-level laws (e.g., Illinois BIPA) for robots collecting facial or voice data. Compliance cost: $300,000–$700,000[5][7].

Total Budget Estimate	
Category	**Estimated Cost (Annual)**
Corporate Measures	$4.35M – $8.5M
Regulatory Development	$12.5M – $25M
Consumer Protections	$4.6M – $9.3M
Total	$21.45M – $42.8M

This proposal balances technical rigor, regulatory oversight, and user empowerment. By aligning with emerging standards like the EU AI Act[4] and FTC guidelines[5], stakeholders can mitigate risks while fostering innovation in the humanoid robotics sector.

Reference

[1] The Threat of Remote Hijacking: Cybersecurity Concerns for Tesla ... https://cybersecurity-magazine.com/the-threat-of-remote-hijacking-cybersecurity-concerns-for-tesla-optimus/

[2] Humanoid Robots: Cybersecurity Concerns And Firewall ... https://vfast.org/journals/index.php/VTSE/article/view/1471

[3] Cyber Security in Robotics Market Outlook & Forecast 2033 https://www.futuremarketinsights.com/reports/cyber-security-in-robotics-market

[4] Robotics at a global regulatory crossroads: compliance challenges ... https://www.osborneclarke.com/insights/robotics-global-regulatory-crossroads-compliance-challenges-autonomous-systems

[5] Cybersecurity Best Practices for AI-Powered Robotics Under State ... https://www.cyberlawmonitor.com/2025/04/21/cybersecurity-best-practices-for-ai-powered-robotics-under-state-and-federal-privacy-laws/

[6] [PDF] Unfair and Deceptive Robots https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4038&context=faculty_scholarship

[7] [PDF] Cybersecurity, safety and robots https://scholarlypublications.universiteitleiden.nl/access/item:3205254/download

[8] Industrial Cybersecurity Budget Alignment: A Manufacturing ... - Elisity https://www.elisity.com/blog/industrial-cybersecurity-budget-alignment-a-manufacturing-framework-guide-for-2025

[9] [PDF] Humanoid Robots and Consumer Law and Policy https://core-prod.cambridgecore.org/core/services/aop-cambridge-core/content/view/4312F04D202AC841F020000B291AE253/9781009386661c39_702-723.pdf/humanoid-robots-and-consumer-law-an

d-policy.pdf
[10] Optimizing Cybersecurity Budgets in 2025: A Strategic Guide https://cymulate.com/blog/cybersecurity-budget-optimization/
[11] Humanoid Robot Market worth $15.26 billion in 2030 - PR Newswire https://www.prnewswire.com/news-releases/humanoid-robot-market-worth-15-26-billion-in-2030---exclusive-report-by-marketsandmarkets-302434062.html
[12] Cyber security of robots: A comprehensive survey - ScienceDirect.com https://www.sciencedirect.com/science/article/pii/S2667305323000625
[13] Humanoids and industrial cybersecurity are driving a surge in ... https://www.cbinsights.com/research/advanced-manufacturing-tech-trends-q1-2024/
[14] Robot startup Figure valued at $2.6 billion by Bezos, OpenAI, Nvidia https://www.cnbc.com/2024/02/29/robot-startup-figure-valued-at-2point6-billion-by-bezos-amazon-nvidia.html
[15] Cybersecurity, safety and robots: Strengthening the link between ... https://www.sciencedirect.com/science/article/pii/S0267364921000017
[16] Industrial Robotics and Cybersecurity: How Manufacturers Can ... https://www.aem.org/news/industrial-robotics-and-cybersecurity-how-manufacturers-can-minimize-risk-and-ensure-safe-operation
[17] Why a Humanoid Robot Makes Sense in Security https://radsecurity.com/why-a-humanoid-robot-makes-sense-in-security/
[18] Special requirements for cybersecurity in robotics - RoboticsBiz https://roboticsbiz.com/special-requirements-for-cybersecurity-in-robotics/
[19] The increasingly regulated development of robotics - The Agility Effect https://www.theagilityeffect.com/en/article/robotics-increasing-regulation-for-enhanced-safety/
[20] Robotic Control System: The Cyber Security Aspects - LinkedIn https://www.linkedin.com/pulse/robotic-control-system-cyber-security-aspects-das-cism-cissp--ypwof
[21] Update on Global AI Regulations: With Great Power Comes Great ... https://thequantumrecord.com/philosophy-of-technology/update-on-global-ai-regulations/
[22] [PDF] Cybersecurity Vulnerabilities in Two Artificially Intelligent ... https://www.ieee-security.org/TC/SPW2019/ConPro/papers/kinzler-conpro19.pdf
[23] Cybersecurity for consumer robots - Electronics360 - GlobalSpec https://electronics360.globalspec.com/article/16895/cybersecurity-for-consumer-robots