1. Record Nr. UNINA9911034947303321

Autore	Harding William
Titolo	Securing a Connected Future : IoT Cybersecurity & IP Security for Makers and Users of Medical Technology / / by William Harding, Andreas Hartmann, Shayla O'Brien, Viktor Sinzig, Gabriel Break, Natalie Sinzig
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-032-07309-X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (174 pages)
Collana	Biomedical and Life Sciences Series
Altri autori (Persone)	HartmannAndreas O'BrienShayla SinzigViktor BreakGabriel SinzigNatalie
Disciplina	610.28
Soggetti	Biomedical engineering Data protection Security systems Big data Database management Artificial intelligence - Data processing Biomedical Devices and Instrumentation Data and Information Security Security Science and Technology Big Data Database Management Data Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1. Understanding the IoT Lifecycle and Associated Cybersecurity Risks -- 2. Cybersecurity Related to IP and Protection of Enterprise Value -- 3. Best Practices for Protecting IP & Ensuring the Security of Medical Devices -- 4. Device Security & Standards -- 5. Digitally Transforming

Manufacturing Operations -- 6. Third-Party Acquisitions: Cybersecurity Risks and Mitigation -- 7. AI Risks to IP, IoT, and Product Management -- 8. Security Trends & The Evolving Digital Landscape -- 9. The Future of Cybersecurity in Medical Devices.

Sommario/riassunto

This book demonstrates how robust cybersecurity measures are essential for protecting intellectual property. By intertwining these two critical areas, the authors aim to provide a unified framework that enhances the security and value of medical technology innovations. With those points in mind, the authors of this book explore the topics of cybersecurity and intellectual property (IP) within the scope of the Internet of Things (IoT) lifecycle, emphasizing medical technology, and providing readers with the knowledge to recognize vulnerabilities at each stage of the IoT and IP development lifecycle. This book thus enables organizations to proactively incorporate robust security measures into their design, development, and protection processes. The topics discussed in this book are (1) protecting sensitive data as it is created, transformed, and aggregated, (2) mitigating potential attacks, (3) the impacts of third-party acquisitions on security, (4) case studies that emphasize potential risks, (5) identification and management of vulnerabilities, and finally (6) examining emerging trends and opportunities associated with integrating new technologies, with an eye toward the future of cybersecurity. This is an essential resource for medical technology R&D leaders, medical technology manufacturing operations leaders, healthcare informaticists, and healthcare industry IP legal teams.