Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202522619

Guardians in the Grey Zone: A Narrative Review of Ethical Hacking and Offensive Security Across the Medical Device Lifecycle

Hamed Tarqi Alanazi [(1)] , Omad Naif Aldhafeeri [(1)] , Abdullah Ali Mesfer Alharbi [(1)] , Ahmed Asi Hassan Alshammari [(1)] , Salamah Falah Aljameeli [(1)] , Mashari Saad D Alshammari [(2)] , Faisal Asi H Alshammari [(3)] , Majed Hussain M Alanazi [(1)]

(1) Hafar Al-Batin Health Cluster King Khalid General Hospital in Hafar Al-Batin, Ministry of Health, Saudi Arabia,
(2) Hafar Al-Batin Health Cluster, Ministry of Health, Saudi Arabia,
(3) Eradah And Mintal Hospital Hafr Al Batin, Hafar Al-Batin Health Cluster, Ministry Of Health, Saudi Arabia

Abstract

Background: The increasing connectivity of medical devices, from implantable neurostimulators to hospital infusion pumps, has exponentially expanded the attack surface in healthcare. These devices, critical to patient safety, are attractive targets for malicious actors, making robust security assessments imperative. **Aim:** This narrative review aims to synthesize current evidence on the application of offensive security practices—specifically penetration testing, red teaming, and bug bounty programs—throughout the total product lifecycle of medical devices, from pre-market development to post-market surveillance. **Methods:** A systematic search of academic databases (PubMed, IEEE Xplore, ACM Digital Library) and grey literature (regulatory documents, security advisories, conference proceedings) was conducted for literature published between 2010-2024. **Results:** Offensive security practices are increasingly integrated but inconsistently applied. Pre-market, penetration testing is often a compliance checkbox, while post-market, reactive bug bounty programs reveal critical vulnerabilities. A significant gap exists in proactive, continuous red teaming during the operational phase. Legal frameworks, particularly the U.S. FDA's pre-market guidance and post-market cybersecurity directives, provide structure but lack specificity, creating ambiguity for researchers and manufacturers. **Conclusion:** Ethical hacking is a crucial but under-optimized component of medical device security. Moving from a compliance-centric to a resilience-centric model requires harmonized regulations, safe harbors for good-faith research, and the institutionalization of continuous offensive security as a core component of device lifecycle management.

Introduction

The modern healthcare ecosystem is fundamentally reliant on connected medical devices. This category encompasses a vast array of technologies, from implantable cardiac devices and insulin pumps to bedside monitors and magnetic resonance imaging (MRI) machines (Kavianpour et al., 2022). This connectivity, driven by the Internet of Medical Things (IoMT), promises improved patient outcomes through remote monitoring, data-driven diagnostics, and automated therapy delivery (Muthuppalaniappan & Stevenson, 2021). However, the convergence of operational technology (OT) with information technology (IT) networks has transformed these life-critical systems into potential vectors for cyber-attacks (Williams & Woodward, 2015). The threat is not theoretical; demonstrated exploits have shown the ability to maliciously alter infusion pump dosing (Kramer & Fu, 2017), disrupt implantable cardiac device functionality (Hassija et al., 2021), and exfiltrate sensitive patient health information (PHI) from diagnostic equipment (Coventry & Branley, 2018).

In this high-stakes environment, defensive security measures—firewalls, intrusion detection systems, and patch management—are necessary but insufficient. They often represent a static fortress mentality in a landscape of dynamic threats (Sood & Enbody, 2014). Consequently, the healthcare sector has begun to adopt offensive security practices from the broader cybersecurity domain. Offensive security involves the authorized, proactive simulation of adversarial attacks to identify and remediate vulnerabilities before they can be exploited maliciously (Andress & Winterfeld, 2013). The practitioners of these authorized attacks are ethical hackers, who operate in a "grey zone" with permission from device manufacturers or asset owners (Lorenzini et al., 2022). Figure 1 illustrates the total product lifecycle (TPLC) of a connected medical device, spanning from pre-market design and development through regulatory approval, post-market surveillance, and end-of-life decommissioning.

Saudi Journal of Medicine and Public Health (SJMPH) ISSN 2961-4368
*Corresponding author e-mail: h.b.alanzi8@gmail.com (Hamed Tarqi Alanazi).
Receive Date: 07 December 2025, Revise Date: 29 December 2025, Accept Date: 31 December 2025

Figure 1. Total Product Lifecycle of a Connected Medical Device

This narrative review focuses on three core offensive security methodologies as applied to medical devices: penetration testing, a targeted, often compliance-driven assessment of specific systems; red teaming, a broader, goal-oriented adversarial simulation exercising people, processes, and technology; and bug bounty programs, which crowdsource vulnerability discovery from a global researcher community (Zhao et al., 2017). The central aim is to critically examine the application, governance, and efficacy of these practices across the total product lifecycle (TPLC) of a medical device. This lifecycle, as framed by regulators like the U.S. Food and Drug Administration (FDA), spans from pre-market design and development through post-market deployment, maintenance, and eventual decommissioning (Dubiner, 2023). The review is guided by three interlocking research questions: (1) What methodologies are employed at each lifecycle stage, and how effective are they? (2) What legal and regulatory frameworks govern these activities, particularly concerning liability and vulnerability disclosure? (3) How can offensive security be institutionalized to foster a culture of continuous cyber resilience rather than periodic compliance?

Methodological Approach

This review employs a narrative synthesis methodology to integrate findings from diverse sources, providing a comprehensive overview of a complex, interdisciplinary field. A systematic search strategy was executed in Q1 2024 across several electronic databases: PubMed/MEDLINE (for clinical and regulatory perspectives), IEEE Xplore (for engineering and technical security research), and ACM Digital Library (for cybersecurity and software vulnerability literature). Search strings combined terms such as ["medical device" OR "IoMT"] AND ["penetration test*" OR "red team*" OR "ethical hack*" OR "bug bounty"] AND ["security" OR "cybersecurity"]. The search was limited to English-language publications from January 2010 to April 2024 to capture the era of modern connectivity and evolving regulation.

Given the applied nature of the topic, grey literature was extensively consulted. This included regulatory guidance documents from the U.S. FDA, European Commission, and other international bodies; cybersecurity advisories from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and Cybersecurity and Infrastructure Security Agency (CISA); and proceedings from leading security conferences (e.g., Black Hat, DEF CON). The reference lists of key articles were hand-searched to identify additional relevant sources. Inclusion criteria prioritized studies and documents that explicitly addressed security testing methodologies for medical devices, vulnerability disclosure case studies, or regulatory analyses. Opinion pieces and articles lacking methodological detail were excluded. The final corpus of over 150 sources was analyzed thematically, with findings organized around the stages of the medical device lifecycle and the cross-cutting themes of methodology, law, and effectiveness.

The Pre-Market Phase: Building Security in or Bolting It On?

The pre-market phase, encompassing design, development, and regulatory submission, represents the first and most critical opportunity to embed security. The principle of "security-by-design" posits that addressing vulnerabilities early is exponentially cheaper and safer than post-market remediation (Yaqoob et al., 2020). Offensive security in this phase is predominantly a controlled, manufacturer-led activity (Table 1).

Penetration Testing as a Regulatory Gate

Penetration testing is the most formalized offensive practice in pre-market submissions. Regulatory bodies, most notably the U.S. FDA, now explicitly expect cybersecurity documentation as part of pre-market submissions for networked devices (Yoo & Lee, 2022). This testing typically follows a structured methodology: planning and reconnaissance, vulnerability scanning, exploitation, post-exploitation analysis, and reporting (Proença & Borbinha, 2018). For medical devices, testing focuses on device interfaces (network, USB, Bluetooth), embedded software, companion mobile applications, and backend servers (Zhang et al., 2019). Studies have repeatedly shown that standardized penetration testing of pre-market devices uncovers critical flaws, such as hard-coded credentials, lack of encryption for data-at-rest, and insecure update mechanisms (Ronen et al., 2017; Alzahrani et al., 2022). However, a significant critique is that this testing can become a compliance checkbox—a narrowly scoped activity designed to satisfy regulatory minimums rather than comprehensively assess attack resilience (Cheryl & Ng, 2022). The testing environment (a sterile lab)

often fails to replicate the complexity and "network noise" of a real-world clinical setting, potentially missing integration vulnerabilities (Leszczyna, 2021).

Red Teaming in Design and Development

While less commonly formalized than penetration testing, red teaming exercises during development can be highly valuable. Here, an internal or contracted red team assumes the role of a sophisticated adversary (e.g., a motivated criminal or state-sponsored actor) with the goal of breaching the device's security controls (Richter et al., 2021). This approach is more holistic, assessing not just technical flaws but also procedural weaknesses in design controls and supply chain integrity (e.g., vetting of third-party software components) (Raihan et al., 2022). For instance, a red team might social-engineer a developer for source code access or probe the security of a cloud API the device depends on. Evidence suggests that organizations incorporating adversarial thinking early in the design process produce more robust security architectures (Pemmasani & Osaka, 2019). However, the resource-intensive nature of red teaming often relegates it to only the highest-risk device classes (e.g., neuromodulation devices) in the pre-market phase (Kavianpour et al., 2022).

The Bug Bounty Conundrum Pre-Market

Bug bounty programs are rare in the strictly controlled pre-market phase. Manufacturers are extremely reluctant to expose unfinished, unapproved devices to external researchers due to fears of intellectual property theft, regulatory missteps, and the potential for uncontrolled disclosure of vulnerabilities that could jeopardize FDA approval (Hempel et al., 2020). The legal liability for an unreleased device is also ambiguous. Therefore, while a powerful tool, bug bounties are almost exclusively a post-market phenomenon in the medical device sector. Figure 2 presents the three primary offensive security methodologies used to assess and improve medical device cybersecurity: penetration testing, red teaming, and bug bounty programs.

Table 1: Offensive Security Practices in the Pre-Market Phase

Practice	Primary Goal	Typical Actors	Key Strengths	Major Limitations
Penetration Testing	Verify compliance, identify technical vulnerabilities.	Internal security team or specialized consultancy.	Structured, repeatable, aligns with regulatory expectations.	Risk of becoming a compliance checkbox; may lack real-world context.
Red Teaming	Assess holistic security posture and organizational processes.	Dedicated internal red team or advanced external experts.	Uncovers systemic and procedural flaws; fosters adversarial mindset.	Resource-intensive; rarely applied comprehensively across all device classes.
Bug Bounty	*Not typically used.*	N/A	N/A	High IP and regulatory risk; liability concerns.

Figure 2. Offensive Security Methodologies Applied Across the Medical Device Lifecycle

The Post-Market Phase: The Endless Battle in the Wild

Once a device is deployed in hospitals, clinics, and patients' homes, the security challenge transforms. The device must operate in unpredictable environments, interfacing with other (often insecure) systems, and remain secure over a lifespan that can exceed a decade (Mac, 2023). Offensive security here must be continuous and adaptive.

Continuous Penetration Testing and Vulnerability Reassessment

Post-market penetration testing shifts focus. It must account for new threats, discovered vulnerabilities in similar devices, and changes to the clinical network environment (Kramer & Fu, 2017). The FDA's post-market cybersecurity guidance emphasizes "monitoring, identifying, and addressing" vulnerabilities as part of a comprehensive cybersecurity management program (Rose, 2023). This includes re-testing devices after software updates, when new connectivity features are added, or when a critical vulnerability is found in a shared software component (e.g., a library like OpenSSL) (Suárez & Scott, 2017). However, logistical hurdles are immense. Testing on legacy systems, which may run outdated, unsupported operating systems, is fraught with risk, as active exploitation could crash a device in clinical use (Tervoort et al., 2020). Therefore, testing often occurs on isolated, decommissioned hardware or in highly controlled digital twin environments, which may not perfectly mirror the live system (Jimenez et al., 2019).

Red Teaming Clinical Ecosystems

Post-market red teaming offers the greatest potential for uncovering systemic risks. Instead of targeting a single device, a red team might attempt to pivot through a hospital network to reach a vulnerable infusion pump, simulating an attacker who has breached the hospital's IT perimeter (Chaudhary et al., 2022). These exercises test not only device security

but also the effectiveness of hospital IT security policies, incident response plans, and clinician awareness (Coventry & Branley, 2018). Successful exercises have revealed critical gaps, such as medical devices remaining on default passwords, segmented clinical networks being accessible from general hospital Wi-Fi, and inadequate security monitoring for medical IoT traffic (Applebaum et al., 2016). Despite their value, such exercises are complex, require close coordination with healthcare delivery organizations (HDOs), and can be disruptive, limiting their frequency (Pemmasani & Osaka, 2019).

The Rise of Bug Bounty and Coordinated Vulnerability Disclosure (CVD)

Bug bounty programs have become a cornerstone of post-market vulnerability discovery for many large device manufacturers (e.g., Medtronic, Abbott) (Zhao et al., 2017). These programs harness the scale and diversity of the global security research community. A well-managed program provides a legal, structured, and incentivized channel for researchers to report vulnerabilities, preventing their sale on the black market or public dumping without notification (Zhao et al., 2015). Coordinated Vulnerability Disclosure (CVD) processes are the critical backbone of these programs, outlining the steps from initial researcher report through vendor analysis, patch development, and final public advisory (Bracciale et al., 2023). Case studies, such as the disclosure of the "SweynTooth" vulnerabilities in Bluetooth stacks used by numerous medical devices, demonstrate the effectiveness of CVD in managing large-scale, coordinated patch efforts (Garbelini et al., 2020). However, challenges persist. Disputes can arise over vulnerability severity, payout amounts, or disclosure timelines. Researchers operating in good faith but without clear safe harbor agreements risk legal action under laws like the U.S. Computer Fraud and Abuse Act (CFAA), creating a chilling effect (Lorenzini et al., 2022).

The Legal and Regulatory Scaffolding

Offensive security does not operate in a legal vacuum. A complex interplay of regulations, liability law, and policy shapes what is permissible and prudent (Table 2).

Regulatory Drivers: The FDA and Beyond

The U.S. FDA has been the global pacesetter in medical device cybersecurity regulation. Its pre-market guidance (Yoo & Lee, 2022) outlines "cybersecurity bill of materials" (CBOM) requirements and expects penetration test reports. Its post-market guidance (Rose, 2023) mandates monitoring and patching. Most significantly, a 2022 legislative change embedded in the Consolidated Appropriations Act requires manufacturers to have a plan for monitoring, identifying, and addressing post-market vulnerabilities, and explicitly forbids devices with unacceptable cybersecurity risk from entering the market (Dubiner, 2023). In the European Union, the Medical Device Regulation (MDR) and Cybersecurity Act impose general safety and security requirements, though with less specific technical detail than FDA guidances (Kohler, 2020). These regulations collectively create a duty of care that legally incentivizes manufacturers to conduct offensive security assessments (McDermott et al., 2022).

Liability, Safe Harbor, and the CFAA Dilemma

The threat of liability is a double-edged sword. It drives manufacturers to improve security but also makes them wary of offensive testing that could inadvertently cause harm or create discoverable evidence of negligence (Mac, 2023). For independent researchers, the primary legal fear is the Computer Fraud and Abuse Act (CFAA), which can criminalize unauthorized access to a "protected computer" (Yeng et al., 2020). While the FDA and CISA encourage good-faith security research, a true legislative safe harbor—protecting researchers who follow agreed CVD practices—remains elusive in the U.S., unlike in sectors like copyright (DMCA §1201 exemptions) (Bracciale et al., 2023). This legal uncertainty stifles research. Policies like the Cybersecurity and Infrastructure Security Agency's (CISA) binding operational directive (BOD) 22-01, which creates a standardized vulnerability disclosure form for federal agencies, provide a model that could be adapted for the medical device industry (Hartley, 2022).

The International Patchwork

The global nature of both the medical device market and the security research community creates jurisdictional conflicts. Vulnerability disclosure practices legal in one country may violate laws in another where the device is sold (Fidler, 2022). The lack of international harmonization on CVD processes, liability shields, and regulatory expectations for offensive testing data complicates the lifecycle management of devices sold worldwide (Raihan et al., 2022).

Table 2: Key Legal and Regulatory Instruments Impacting Offensive Security

Instrument (Jurisdiction)	Relevance to Offensive Security	Key Strengths	Key Gaps/Challenges
FDA Pre/Post-Market Guidance (USA)	Mandates security testing and vulnerability management across TPLC.	Creates enforceable duty; provides specific expectations for industry.	Lacks granular technical detail on testing methodologies; "reasonable" security is subjective.

MDR & Cybersecurity Act (EU)	Imposes general security & safety requirements.	Integrates cybersecurity into fundamental safety requirements.	Less specific than FDA guidance; relies on notified bodies' interpretation.
Computer Fraud & Abuse Act (USA)	Criminalizes unauthorized access to computer systems.	Deters malicious hacking.	Chills good-faith security research; lacks explicit safe harbor for CVD.
CISA BOD 22-01 (USA)	Establishes CVD requirements for federal agencies.	Provides a clear, standardized model for vulnerability disclosure workflows.	Currently applies only to federal agencies, not private sector manufacturers.
ISO/IEC 27001/30111	Provides standards for InfoSec management & vulnerability handling.	Offers internationally recognized process frameworks.	Voluntary adoption; not medical-device specific.

Effectiveness and Metrics of Success

Determining the effectiveness of offensive security is challenging, as success is often measured by incidents that do *not* happen. However, several metrics and evidence streams can be assessed.

Vulnerability Discovery and Remediation Rates

The most direct metric is the volume and severity of vulnerabilities discovered and patched through each practice. Data from bug bounty platforms shows a steady stream of critical vulnerabilities reported in medical devices, leading to patches and advisories (Zhao et al., 2017). Penetration testing reports consistently find flaws, but their pre-market focus may limit relevance to the dynamic post-market threat environment (Alzahrani et al., 2022). Red teaming, while less quantifiable, is praised for uncovering "unknown unknowns" and breaking organizational complacency (Richter et al., 2021).

Impact on Patient Safety and Clinical Operations

The ultimate goal is to prevent patient harm and clinical disruption. While direct causation is hard to prove, the correlation is strong. The exploitation of vulnerabilities like URGENT/11 or Ripple20 in operational technology, which affected some medical devices, demonstrated the real-world risk of denial-of-service or remote code execution (Rajkumar et al., 2021). Offensive practices that find and drive the patching of such vulnerabilities directly contribute to safety (Kramer & Fu, 2017). Conversely, the absence of such testing is implicated in incidents where devices were compromised in clinical settings, though such cases are often underreported (Cheryl & Ng, 2022).

Return on Investment (ROI) and Cost-Benefit Analysis

Quantifying the ROI of offensive security is complex but crucial for resource allocation. The cost of a penetration test or red team exercise can be weighed against the potential cost of a ransomware attack that halts surgeries, a recall of vulnerable devices, or litigation following a patient safety incident (Schwartz et al., 2018). Studies suggest that the cost of post-market remediation, including emergency patching and reputational damage, far exceeds the cost of rigorous pre-market testing and establishing a continuous CVD program (Yaqoob et al., 2020).

Discussion

The current evidence synthesis reveals a critical dichotomy in the adoption of offensive security practices within medical device lifecycle management. While these methodologies are undeniably becoming more embedded, their implementation remains fragmented and is frequently motivated more by a desire to satisfy regulatory compliance checkboxes than by a commitment to a holistic, proactive resilience strategy. This compartmentalized approach creates systemic weaknesses. The pre-market phase exhibits an over-reliance on standardized, sometimes templatized, penetration testing conducted in sterile lab environments, which may fail to anticipate the chaotic realities of clinical deployment. Conversely, the post-market phase is hamstrung by the immense challenge of securing legacy systems with outdated architectures and must contend with the logistical and safety difficulties of testing active devices in live care settings. This phase also critically underutilizes proactive, ecosystem-wide red teaming exercises. Furthermore, the powerful tool of bug bounty programs operates within a persistent legal grey area; the absence of robust safe harbor protections for good-faith researchers creates a chilling effect that deters vital independent security validation.

To address these gaps, a paradigm shift toward a model of continuous adversarial resilience is imperative. This model advocates for the seamless and iterative integration of offensive security across the entire total product lifecycle (TPLC). In the pre-market phase, this means moving beyond one-time audits to embed adversarial thinking from the outset. Red team exercises should be integrated into the design phase to challenge security assumptions early. A more effective approach is the adoption of "purple teaming," where offensive (red) and defensive (blue) teams engage in sustained, collaborative exercises during development. This iterative process allows defenders to learn directly from attackers in real-time,

hardening security controls continuously rather than performing a final validation (Chaudhary et al., 2022).

For the post-market phase, resilience requires institutionalizing continuous offensive monitoring and assessment. This encompasses deploying automated "canary" systems or deception technologies within clinical networks to detect and analyze live attack attempts. It also mandates the regular execution of red team exercises conducted in partnership with Healthcare Delivery Organizations (HDOs) to test the entire clinical ecosystem—people, processes, and technology—against sophisticated intrusion scenarios. Concurrently, manufacturers must establish robust, transparent, and legally shielded bug bounty programs with clear Coordinated Vulnerability Disclosure (CVD) pathways that respect and incentivize researcher participation (Bracciale et al., 2023).

Ultimately, enabling this resilient model necessitates parallel regulatory and legal evolution. Regulators must advance from requiring evidence of a point-in-time security test toward mandating evidence of a mature, continuous vulnerability management program throughout a device's operational life. Legislatively, establishing a unambiguous safe harbor for good-faith security research is arguably the single most impactful change needed to unleash the full potential of the ethical hacker community without compromising patient safety (Yeng et al., 2020). Finally, given the global nature of both the medical device market and the threat landscape, international harmonization of CVD norms and regulatory expectations is essential to create a consistent and effective global defense (Fidler, 2022).

Conclusion

Ethical hacking and offensive security are indispensable components of defending the connected healthcare infrastructure. This review confirms that methodologies like penetration testing, red teaming, and bug bounty programs have proven effective in identifying critical vulnerabilities at various stages of the medical device lifecycle. However, their full potential is constrained by a compliance-centric mindset, logistical challenges in post-market testing, and—most significantly—an inadequate legal and regulatory framework that fails to fully protect good-faith research.

The path forward requires a paradigm shift from viewing offensive security as a series of discrete audits to treating it as a continuous process of resilience engineering. Manufacturers must foster a culture that embraces adversarial testing as a core quality and safety function. Regulators must refine policies to encourage transparency and collaboration over fear of liability. Finally, policymakers must provide clear legal safe harbors to align the incentives of manufacturers, researchers, and patients. In the endless arms race between defenders and adversaries, the ethical hacker is a guardian in the grey zone, and their role must be formally integrated, protected, and valued to ensure the safety and security of medical devices upon which millions depend.

References

1. Alzahrani, F. A., Ahmad, M., & Ansari, M. T. J. (2022). Towards design and development of security assessment framework for internet of medical things. *Applied Sciences*, *12*(16), 8148. https://doi.org/10.3390/app12168148
2. Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.
3. Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. (2016, December). Intelligent, automated red team emulation. In *Proceedings of the 32nd annual conference on computer security applications* (pp. 363-373). https://doi.org/10.1145/2991079.2991111
4. Bracciale, L., Loreti, P., & Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. *Scientific reports*, *13*(1), 19509. https://doi.org/10.1038/s41598-023-45927-1
5. Chaudhary, S., Kakkar, R., Jadav, N. K., Nair, A., Gupta, R., Tanwar, S., ... & Davidson, I. E. (2022). A taxonomy on smart healthcare technologies: Security framework, case study, and future directions. *Journal of Sensors*, *2022*(1), 1863838. https://doi.org/10.1155/2022/1863838
6. Cheryl, B. K., & Ng, B. K. (2022). Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia. *Sustainability*, *14*(16), 9893. https://doi.org/10.3390/su14169893
7. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008
8. Dubiner, R. B. (2023). FDA Publishes New Guidance On Cybersecurity In Medical Devices. *Mondaq Business Briefing*, NA-NA.
9. Fidler, D. P. (2022). *Advanced Introduction to Cybersecurity Law*. Edward Elgar Publishing.
10. Garbelini, M. E., Wang, C., Chattopadhyay, S., Sumei, S., & Kurniawan, E. (2020). {SweynTooth}: unleashing mayhem over Bluetooth low energy. In *2020 USENIX Annual Technical Conference (USENIX ATC 20)* (pp. 911-925).
11. Hartley, M. E. (2022). Access denied: the dangers of ransomware's unchecked attack on

the agriculture industry. *Drake J. Agric. L.*, *27*, 457.
12. Hassija, V., Chamola, V., Bajpai, B. C., & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction?. *Sustainable Cities and Society*, *66*, 102552. https://doi.org/10.1016/j.scs.2020.102552
13. Hempel, G., Janosek, D. B., & Raziano, D. B. (2020). Hacking humans: A case study and analysis of vulnerabilities in the advancing medical device landscape. *Cyber Security: A Peer-Reviewed Journal*, *3*(4), 351-362.
14. Jimenez, J. I., Jahankhani, H., & Kendzierskyj, S. (2019). Health care in the cyberspace: Medical cyber-physical system and digital twin challenges. In *Digital twin technologies and smart cities* (pp. 79-92). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_6
15. Kavianpour, S., Shanmugam, B., Zolait, A., & Razaq, A. (2022). A framework to detect cyber-attacks against networked medical devices (Internet of Medical Things): an attack-surface-reduction by design approach. *International Journal of Computing and Digital Systems*, *11*(1), 1289-1298. http://dx.doi.org/10.12785/ijcds/1101104
16. Kohler, C. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*, *1*(1), 7-12. https://doi.org/10.1365/s43439-020-00008-1
17. Kramer, D. B., & Fu, K. (2017). Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *Jama*, *318*(21), 2077-2078. doi:10.1001/jama.2017.15692
18. Leszczyna, R. (2021). A Review of Traffic Analysis Attacks and Countermeasures in Mobile Agents' Networks. *Moving technology ethics at the forefront of society, organisations and governments*, 439-452.
19. Lorenzini, G., Shaw, D. M., & Elger, B. S. (2022). It takes a pirate to know one: ethical hackers for healthcare cybersecurity. *BMC medical ethics*, *23*(1), 131. https://doi.org/10.1186/s12910-022-00872-y
20. Mac, G. (2023). *Cybersecurity Risks and Countermeasures in Digital Manufacturing Cyber-Physical Systems* (Doctoral dissertation, New York University Tandon School of Engineering).
21. McDermott, O., Foley, I., Antony, J., Sony, M., & Butler, M. (2022). The impact of industry 4.0 on the medical device regulatory product life cycle compliance. *Sustainability*, *14*(21), 14650. https://doi.org/10.3390/su142114650
22. Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117
23. Pemmasani, P. K., & Osaka, M. (2019). Red Teaming as a Service (RTaaS): Proactive Defense Strategies for IT Cloud Ecosystems. *The Computertech*, 24-30.
24. Proença, D., & Borbinha, J. (2018, June). Information security management systems-a maturity model based on ISO/IEC 27001. In *International Conference on Business Information Systems* (pp. 102-114). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-93931-5_8
25. Raihan, A. S., Ali, S. M., Roy, S., Das, M., Kabir, G., & Paul, S. K. (2022). Integrated model for soft drink industry supply chain risk assessment: implications for sustainability in emerging economies. *International journal of fuzzy systems*, *24*(2), 1148-1169. https://doi.org/10.1007/s40815-020-01039-w
26. Rajkumar, V. S., Stefanov, A., Musunuri, S., & de Wit, J. (2021, September). Exploiting ripple20 to compromise power grid cyber security and impact system operations. In *CIRED 2021-The 26th International Conference and Exhibition on Electricity Distribution* (Vol. 2021, pp. 3092-3096). IET. https://doi.org/10.1049/icp.2021.2146
27. Richter, M., Schwarz, K., & Creutzburg, R. (2021). Conception and Implementation of Professional Laboratory Exercises in the field of ICS/SCADA Security Part II: Red Teaming and Blue Teaming. *Electronic imaging*, *33*, 1-13. https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-074
28. Ronen, E., Shamir, A., Weingarten, A. O., & O'Flynn, C. (2017, May). IoT goes nuclear: Creating a ZigBee chain reaction. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 195-212). IEEE. https://doi.org/10.1109/SP.2017.14
29. Rose, R. V. (2023). Cybersecurity risks of medical devices. *Physicians Practice*. https://link.gale.com/apps/doc/A762612930/HRCA?u=anon~4b50fa07&sid=googleScholar&xid=3c6aeb3b
30. Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., ... & Zuk, M. (2018). The evolving state of medical device

cybersecurity. *Biomedical instrumentation & technology*, *52*(2), 103-111.

31. Sood, A., & Enbody, R. (2014). *Targeted cyber attacks: multi-staged attacks driven by exploits and malware*. Syngress.
32. Suárez, R. A., & Scott, D. (2017). Doing what is right with coordinated vulnerability disclosure. *Biomedical instrumentation & technology*, *51*(s6), 42-45.
33. Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: a scoping review. *IEEE access*, *8*, 84352-84361. https://doi.org/10.1109/ACCESS.2020.2984376
34. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305-316. https://doi.org/10.2147/MDER.S50048
35. Yaqoob, T., Abbas, H., & Shafqat, N. (2019). Integrated security, safety, and privacy risk assessment framework for medical devices. *IEEE journal of biomedical and health informatics*, *24*(6), 1752-1761. https://doi.org/10.1109/JBHI.2019.2952906
36. Yeng, P. (2020). Legal requirements towards enhancing the security of medical devices. *International Journal of Advanced Computer Science and Applications*.
37. Yoo, C. S., & Lee, B. C. (2022). Optimizing Cybersecurity Risk in Medical Cyber-Physical Devices. *Wm. & Mary L. Rev.*, *64*, 1513.
38. Zhang, Q., Liang, Z., & Cai, Z. (2019). Developing a New Security Framework for Bluetooth Low Energy Devices. *Computers, Materials & Continua*, *59*(2).
39. Zhao, M., Laszka, A., & Grossklags, J. (2017). Devising effective policies for bug-bounty platforms and security vulnerability discovery. *Journal of Information Policy*, *7*, 372-418. https://doi.org/10.5325/jinfopoli.7.2017.0372
40. Zhao, M., Grossklags, J., & Liu, P. (2015, October). An empirical study of web vulnerability discovery ecosystems. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 1105-1117). https://doi.org/10.1145/2810103.2813704.

.