TORRENS UNIVERSITY AUSTRALIA

From Credential to Catastrophe:

IoT and Cloud Security Through the Lens of the Stryker 2026 Cyber-attack

Student: Jose Antonio Escalante Lopez
Student ID: A00154979
Course: ICD542 IoT, Cloud and Digital Infrastructure Protection
Date: 2026-04-19
Assessment Type: Report

https://orcid.org/0009-0000-5896-6797
openpgp4fpr:bb5b08bd40c6bd27cf4e68a4b24525ef85e6a3ba

Table of Contents

1 Abstract 3
2 IoT, Cloud Computing and Digital Infrastructure 3
3 IoT Technologies 3
4 Cloud Technologies 4
5 IoT Governance 4
6 Conclusion 5
References 5
7 Technical Appendix 6
7.1 Appendix A — IoTWF Reference Model Attack Mapping 6
7.2 Appendix B — IoT Cyber Risk Management Framework 6

1 Abstract

The rapid convergence of Internet of Things and cloud technologies has created a digital infrastructure that underpins critical services globally. This report examines the fundamental concepts, security challenges and countermeasures associated with these technologies, using the March 2026 Stryker Corporation cyberattack as a central case study. The attack — executed through a single stolen credential without malicious code — demonstrates systemic vulnerabilities inherent in interconnected digital infrastructure. The report argues that technical countermeasures such as FIDO2 authentication and least privilege governance, combined with structured risk management frameworks, are essential to securing modern IoT and cloud environments.

2 IoT, Cloud Computing and Digital Infrastructure

The Internet of Things (IoT) describes the interconnection of physical devices across networks, enabling data collection and exchange at an unprecedented scale (Sinclair, 2017). As illustrated in Figure 1, the number of connected devices reached 21.1 billion in 2025 and is projected to grow exponentially over the next decade (Sinha, 2025). Cloud computing amplifies this by providing the storage, processing power and intelligence that transforms raw device data into actionable outcomes (Rejeb et al., 2022). Together with communication protocols and physical hardware, these layers form what is known as digital infrastructure. These technologies deliver measurable benefits from improved patient care and operational efficiency to scalable, on-demand computing for businesses globally. However, the March 2026 cyberattack on Stryker Corporation where a single stolen credential enabled hacktivists to wipe 200,000 devices and exfiltrate 50 terabytes of data across 61 countries (Alder, 2026) illustrates the systemic risk this convergence creates. This report examines the fundamental concepts of IoT and cloud technologies, the cybersecurity challenges they present, and the countermeasures required to protect them.

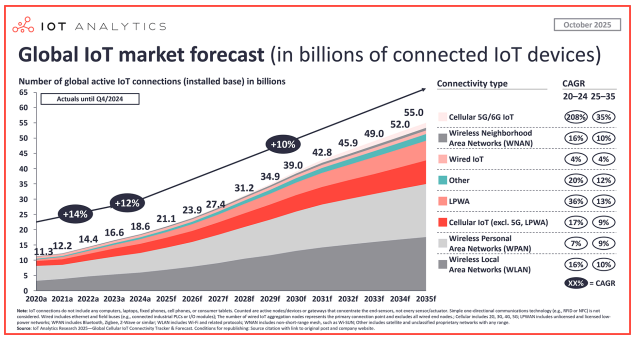

Figure 1: (Sinha, 2025)

3 IoT Technologies

Thinking about IoT as anything, anywhere, anytime summarized a complex concept that is integrated by several elements. The Figure 2 illustrates how IoT is composed essentially with the Stryker Cyberattack incident as an example.

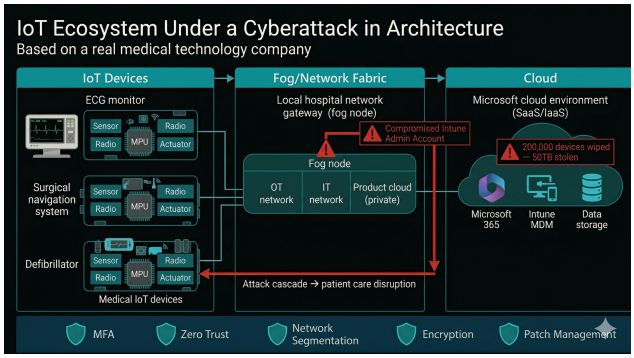

Figure 2: (Jones, 2026) Gemini

IoT implies in its concept physical, network, business, cloud and data elements that works interconnected with the major purpose of information as stated by Kiran (2019).

> The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. (Kiran, 2019)

Familiar examples include consumer ecosystems such as Apple, where devices, platforms and applications operate as a unified network, and Stryker, which evolved traditional medical equipment into Software Defined Products; intelligent, connected devices that collect and transmit patient data in real time (Stryker, n.d.).

Despite the transformative potential IoT offers, significant challenges emerge when deploying

these products at scale. The Stryker cyberattack demonstrates that gaining access to core network credentials allows attackers to control connected devices and exfiltrate data freely (Alder, 2026), reflecting the sixth and eighth risks identified by OWASP Foundation (n.d.) insufficient privacy protection and lack of physical hardening respectively.

4 Cloud Technologies

Cloud technologies, particularly cloud computing and storage, are essential to IoT ecosystems. The *"anything, anywhere, anytime"* principle is only achievable because both work together: IoT devices generate data and cloud platforms process it to extract patterns, statistics and insights that feed AI models, broadening IoT applications (Rivers, 2022).

> "As a service" refers to the way IT assets are consumed with cloud-based products, highlighting the essential difference between cloud computing and traditional IT. (IBM, n.d.)

As IBM (n.d.) establishes, cloud computing delivers IT resources through three core service models. Infrastructure as a Service (IaaS) provides on-demand access to virtualised compute, storage and networking resources (IBM, n.d.). Platform as a Service (PaaS) extends this with pre-configured environments and tools such as GitHub Actions enabling development without managing underlying infrastructure (Rivers, 2022). Software as a Service (SaaS) delivers fully operational applications via the internet, such as Microsoft 365 or Salesforce (IBM, n.d.). IoT ecosystems rely on all three models, making cloud security inseparable from IoT security (Rivers, 2022). This dependency was critical in the Stryker cyberattack, where Microsoft Intune a SaaS device management platform was weaponised through a compromised administrator account to remotely wipe 200,000 endpoints globally (Jones, 2026). The incident exposes a fundamental challenge: organizations frequently misunderstand the shared responsibility model, assuming cloud providers secure all layers when identity and access management remain the customer's responsibility (IBM, n.d.).

5 IoT Governance

Understanding the IoT architecture within the OSI model benefits cybersecurity professionals regarding tools, standards and frameworks applicable in practical environments. Listing instruments or measures alone does not contribute to a meaningful application of them within real case studies. The Stryker cyberattack is a case study with critical consequences where no malicious code or exploitable vulnerability was deployed, yet the attackers gained access regardless. Analyzing the IoT architecture it is possible to map the attack as shown in Figure 3. The event started at the top of the architecture (El Hakim, 2018) in the Collaboration and Processes layer through a stolen administrator credential. Nevertheless, the real attack executed at the Application layer where countermeasures such as **Multi-Factor Authentication** particularly FIDO2 (Suleski et al., 2023), which binds authentication to a physical device could have prevented further propagation (National Institute of Standards and Technology, 2024). The attack then spread through a Microsoft Intune administrator credential with unrestricted VPN network access, where a least privilege policy administered through Active Directory could have prevented further escalation. Finally, when an unusual volume of simultaneous requests was issued, a multi-party authorization (Al-Aqrabi et al., 2024) requirement could have minimized the critical actions of the attackers.

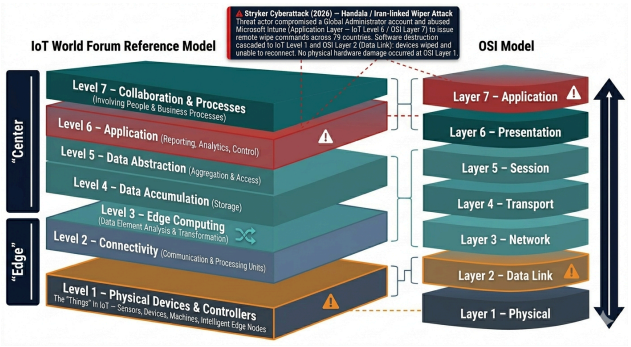

Figure 3: (El Hakim, 2018), (International Organization for Standardization & International Electrotechnical Commission, 2022), Gemini

Furthermore, the most concerning implication of the attack was the absence of a *Risk Management Plan*. Stryker appeared to have no mitigation plan for such an event no guidelines, no framework. Stryker should strengthen their *Risk Management*

Plan in accordance with International Organization for Standardization & International Electrotechnical Commission (2022) and Lee (2020), where at the IoT Cyber Risk Assessment Layer the organization should identify future cyber risks across three core activities: risk identification, risk quantification and resource allocation. This critical layer within Lee (2020) framework was absent at Stryker, illustrating the importance of clear governance frameworks and proactive countermeasures.

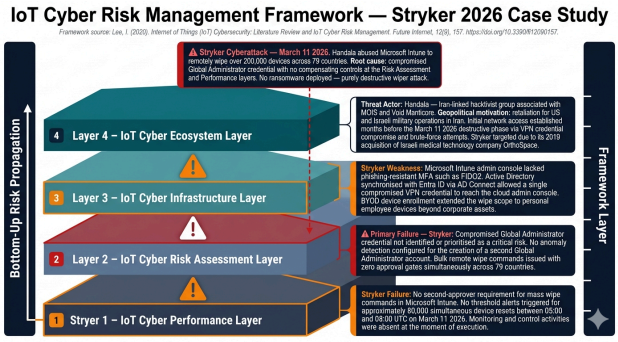

Figure 4: (Lee, 2020) Gemini

6 Conclusion

IoT and cloud technologies have been shaping a more connected world without borders, driving new technologies and amplifying the human experience. Ironically, this deeply interconnected world can be disrupted as easily as a single credential being compromised as Stryker demonstrated, everything that relies on shared network infrastructure and cloud services is only as resilient as its weakest access point.

References

Al-Aqrabi, H., Manasrah, A. M., Hill, R., Shatnawi, M. Q., Daoud, M. S., & Alkhzaimi, H. (2024). Dynamic Authentication for Intelligent Sensor Clouds in the Internet of Things. *International Journal of Information Security*, *23*(3), 2003–2021. https://doi.org/10.1007/s10207-024-00829-9

Alder, S. (2026, March 20). *Iran linked hacking group wipes data of U.S. medical device manufacturer*. https://www.hipaajournal.com/stryker-cyberattack-iran/

El Hakim, A. (2018). *Internet of Things (IoT) System Architecture and Technologies* [Technical report]. https://doi.org/10.13140/RG.2.2.17046.19521

IBM. (n.d.). *IaaS, PaaS, SaaS: What's the difference?*. https://www.ibm.com/think/topics/iaas-paas-saas

International Organization for Standardization, & International Electrotechnical Commission. (2022). *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements* (Technical Report No. ISO/IEC27001:2022). https://www.iso.org/standard/27001

Jones, D. (2026, March 16). *Stryker attack raises concerns about role of device management tool*. https://www.cybersecuritydive.com/news/stryker-attack-device-management-microsoft-iran/814816/

Kiran, D. (2019). Chapter 35 - Internet of Things. In D. Kiran (Ed.), *Production Planning and Control: Production Planning and Control* (pp. 495–513). Butterworth-Heinemann. https://doi.org/https://doi.org/10.1016/B978-0-12-818364-9.00035-4

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*, *12*(9), 157. https://doi.org/10.3390/fi12090157

National Institute of Standards and Technology. (2024). *Digital Identity Guidelines: Authentication and Lifecycle Management* (Technical Report Nos. SP800–63B). https://pages.nist.gov/800-63-4/sp800-63b.html

OWASP Foundation. (n.d.). *OWASP Internet of Things Project*. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H., & Zailani, S. (2022). The big picture on the internet of things and the smart city: a review of what we know and what we need to know. *Internet of Things*, *19*, 100565. https://doi.org/10.1016/j.iot.2022.100565

Rivers, D. (2022, May 13). *Introduction to Cloud Computing for IT Pros*. https://www.linkedin.com/learning/introduction-to-cloud-computing-for-it-pros-17408371

Sinclair, B. (2017, June). *IoT Foundations: Fundamentals*. https://www.linkedin.com/learning/iot-foundations-fundamentals

Sinha, S. (2025, October 28). *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally*. https://iot-analytics.com/number-connected-iot-devices/

Stryker. (n.d.). *Our history*. https://www.stryker.com/au/en/about/history.html

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*, 1–20. https://doi.org/10.1177/20552076231177144

7 Technical Appendix

7.1 Appendix A — IoTWF Reference Model Attack Mapping

Figure 3 illustrates the mapping of the Stryker 2026 cyberattack against the IoT World Forum Reference Model and OSI Model, showing how the attack originated at Level 7 and cascaded to Level 1.

7.2 Appendix B — IoT Cyber Risk Management Framework

Figure 4 applies the framework proposed by Lee (2020) to the Stryker 2026 case study, identifying specific failures at each layer of the IoT Cyber Risk Management Framework.