
LYNN
UNIVERSITY

# Evolving Cybersecurity Landscape for Luxury and Fashion Houses: A Proactive Approach to Protecting Digital Assets and Gaining Competitive Advantage

Dr. George Antoniou
Associate Professor, Cyber Security
College of Business and Management
Lynn University

Dr. Andrew Burnstine
Associate Professor, Fashion
College of Business and Management
Lynn University

LYNN UNIVERSITY

# Agenda

LYNN UNIVERSITY

# Introduction

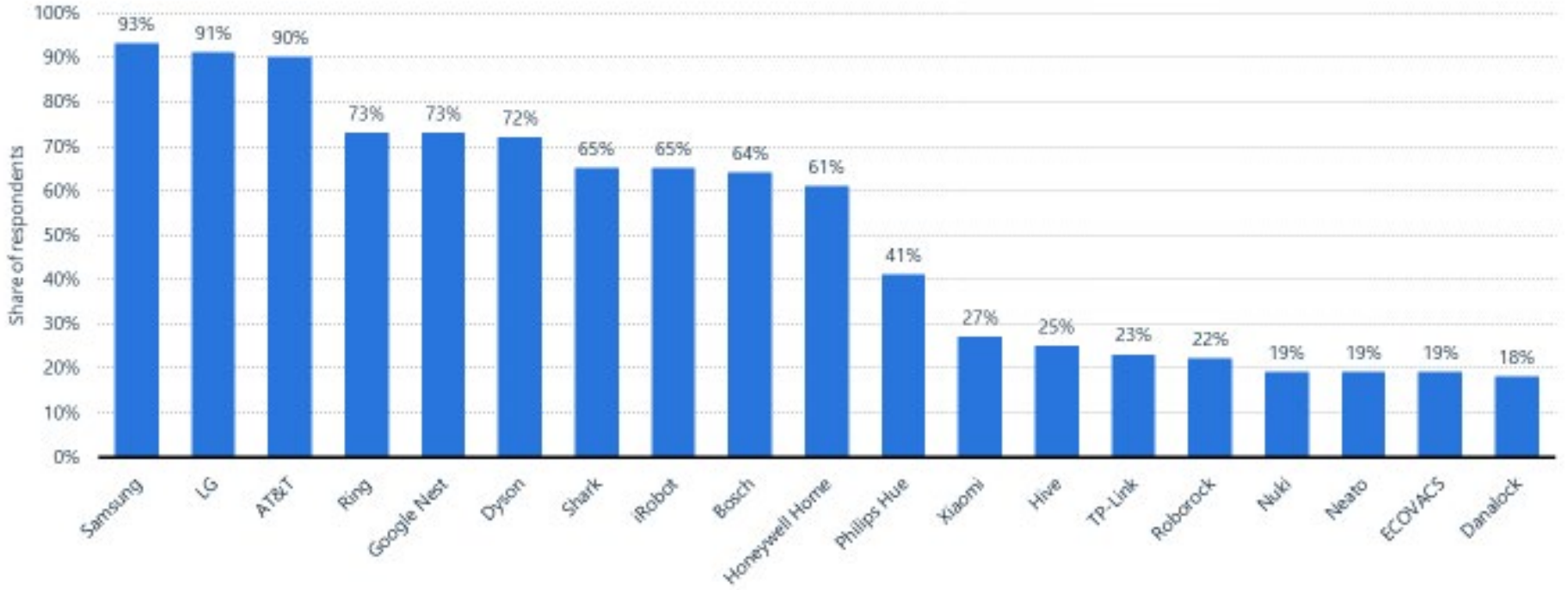
- Digital transformation increases reliance on digital technology, including IoT and smart homes
- Luxury and fashion industries face new cybersecurity challenges
- Growing reliance on digital technology in luxury and fashion industries
- Increased vulnerability to cyber threats
- Importance of protecting digital assets and intellectual property
- Protecting digital assets and intellectual property is crucial

# IoT and Smart Homes in Luxury and Fashion

- IoT and smart homes offer numerous automation opportunities
- Luxury and fashion industries embrace IoT technology for personalized customer experiences
- Increased connectivity creates new cybersecurity risks

## Leading smart home brands ranked by brand awareness in the United States in 2022

Most well-known smart home brands in the United States 2022




4

**Note(s):** United States; August 2022; 18 to 64 years; 1249 respondents
Further information regarding this statistic can be found on page 8.
**Source(s):** Statista Consumer Insights; ID 1341441

statista

LYNN UNIVERSITY

# What's the Internet of Things

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts".

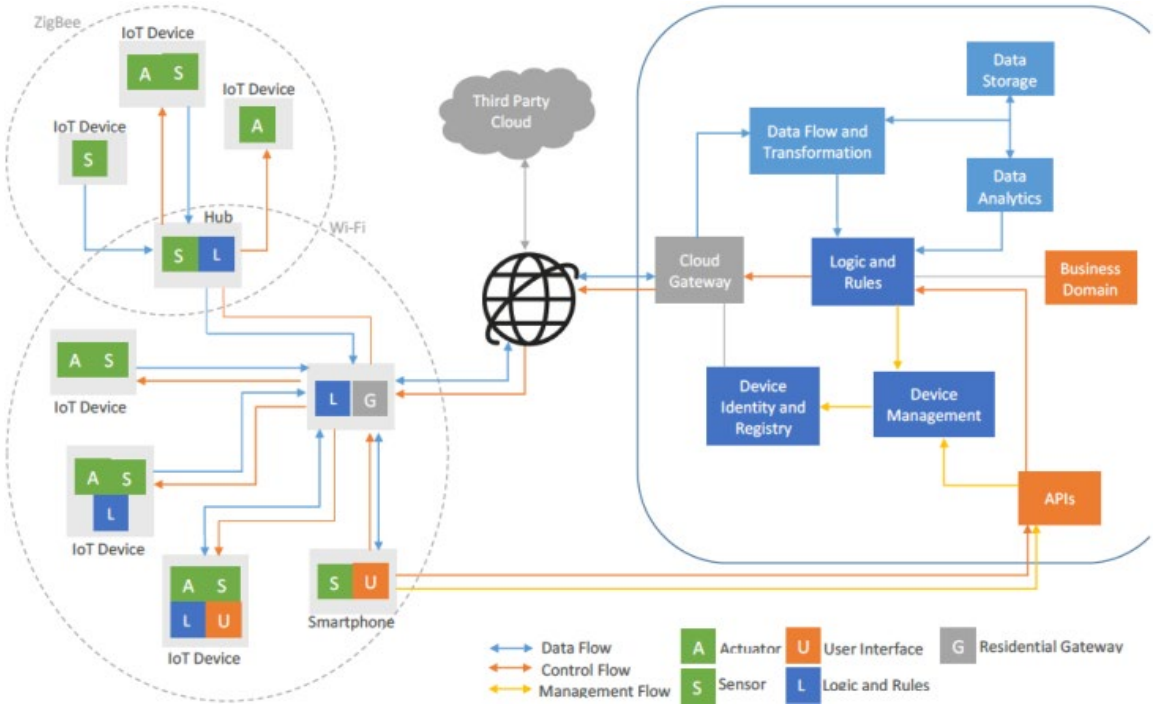
-------IoT in 2020

LYNN UNIVERSITY

# Application of IoT in Fashion Luxury Smart Homes

Examples:

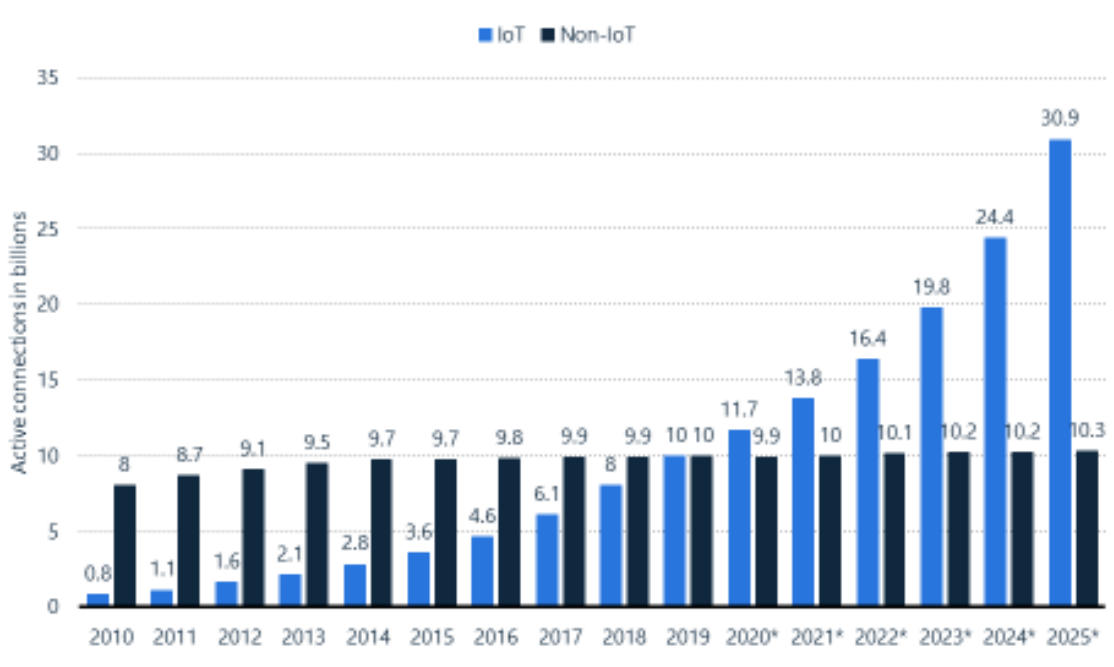
- Wireless Charging
- The Advent of Biometric Security
- The Smarter Kitchen
- The State-of-the-Art Personal Assistant
- Energy Efficient and Self-Sustaining
- Video Doorbells
- Smart Gardening
- Smart Heating
- Door Locks




Note: Smart Home architecture example with the three viewpoints merged. Adapted from: Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: development of a reference architecture for attack surface analysis. IoT.

## Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 (in billions)

IoT and non-IoT connections worldwide 2010-2025




**Your Headline**

Your Notes:

**Note(s):** Worldwide; 2015 to 2019

Further information regarding this statistic can be found on page 8.

**Source(s):** IoT Analytics; ID 1101442

statista

LYNN UNIVERSITY

# Problem Statement

- Risks of cyber-attacks due to reliance on digital technology use in Luxury Fashion Homes
- Luxury and fashion Homes face unique cybersecurity challenges with IoT and smart homes
  Consequences: financial loss, reputational damage, operational disruption, identity theft
- Need for a proactive cybersecurity approach to navigate cybersecurity landscape in luxury fashion smart homes and to maintain individual's privacy
- In 2019, thirty-five percent of U.S. households with broadband faced security issues as smart doorbells and other security devices were hacked.

LYNN UNIVERSITY

# Luxury Smart Homes Concerns

- The Functional Viewpoint:
  concerned with the functions that enable IoT devices, their structure and interactions.
- The Physical Viewpoint:
  concerned with the physical components of the of the Smart Home ecosystem.
- The Communication Viewpoint:
  concerned with the technologies that enable devices and cloud platforms to interact

LYNN UNIVERSITY

# Recommended Solutions

- Conduct regular risk assessments, including IoT devices
- Implement robust security measures for IoT-enabled systems
- Foster a culture of cybersecurity with a focus on IoT and smart home technologies
- Collaborate with cybersecurity experts to address IoT-specific risks

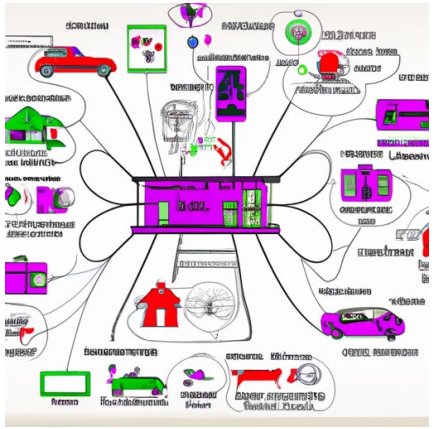
LYNN UNIVERSITY

# Regulations
# Luxury Fashion Homes and IoT

- Luxury and fashion houses must adhere to key regulations, including IoT-specific guidelines
- General Data Protection Regulation (GDPR) in the EU
- California Consumer Privacy Act (CCPA)
- IoT security standards and frameworks, such as NIST guidelines for IoT

LYNN UNIVERSITY

# Conclusion



- Luxury and fashion houses must navigate the evolving cybersecurity landscape
- Navigating evolving cybersecurity landscape is critical, especially with the growth of IoT and smart homes
- Importance of risk assessments, security measures, culture, and collaboration
- Adherence to regulations can help safeguard privacy and security
- Implementing solutions can protect digital assets and ensure privacy

# Questions and Discussion

Thank you for your attention.
Let's open the floor for questions and discussion about the research findings and recommendations.

Please share your thoughts, insights, and experiences related to cybersecurity in the luxury and fashion industries, with a focus on smart homes.