Cyber Resilience

Mango Wearable Solutions

Why is Cybersecurity Critical?

CYBERSECURITY THREATS

- EXTERNAL HACKING 50%
- MALWARE 46%
- PHYSICAL SECURITY ATTACKS 18%
- 20% MOBILE DEVICE THEFT
- 37% SOCIAL ENGINEERING
- 25% DENIAL OF SERVICE
- 29% INSIDER DATA LEAKAGE/THEFT
- 36% SPAM

Federal Virtual Training Environment
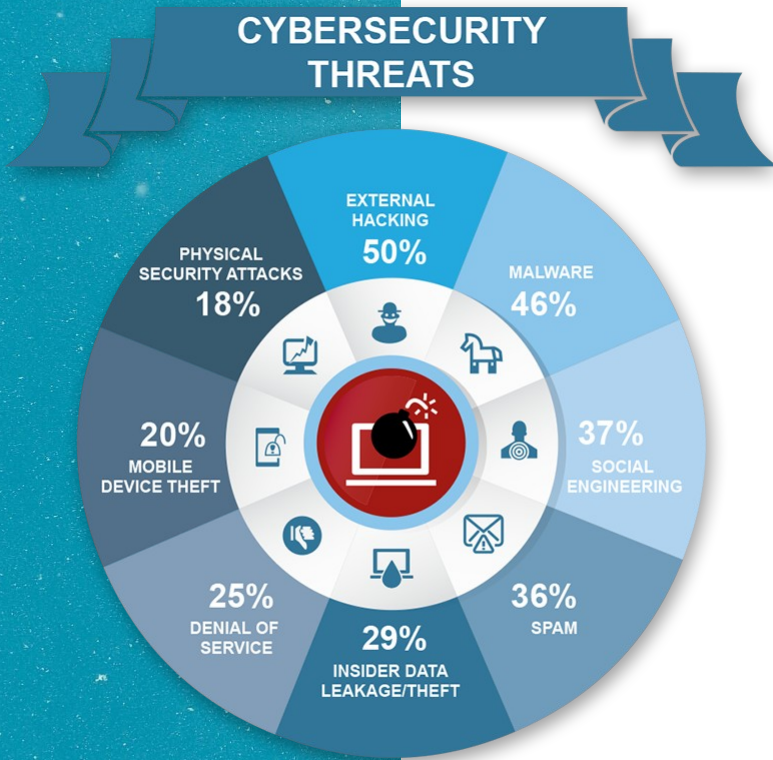
- Cyberattacks threaten every industry

- These attacks can lead to reputational , legal, and financial damage

- These all cause severe operational disruptions

- All of these attacks are more significant for Mango WS

How Does This Affect Mango WS?

- Protection of Physical Data

Intellectual Property Theft
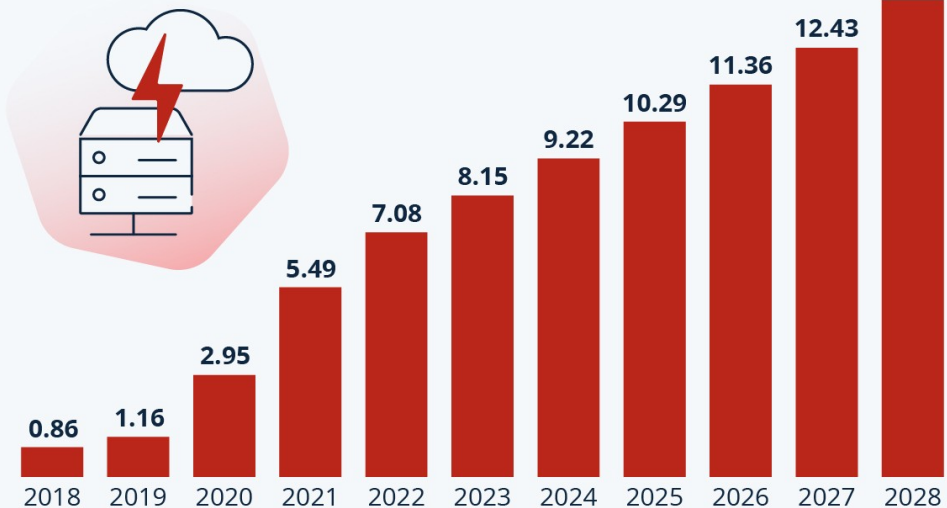
- Regulatory Scrutiny

Our Mission

The stakes for cybersecurity at Mango Wearable Solutions are far higher than in many other industries. It's not just about protecting business data—it's about safeguarding lives, meeting regulatory standards, and preserving trust in cutting-edge healthcare technology.

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide
(in trillion U.S. dollars)

Year	Value
2018	0.86
2019	1.16
2020	2.95
2021	5.49
2022	7.08
2023	8.15
2024	9.22
2025	10.29
2026	11.36
2027	12.43
2028	13.82

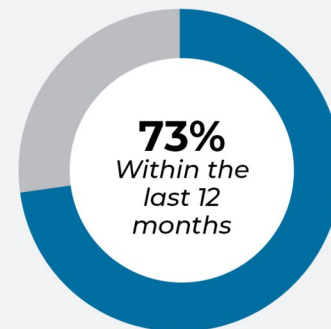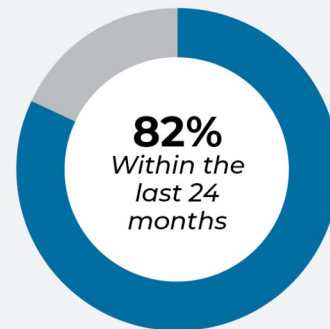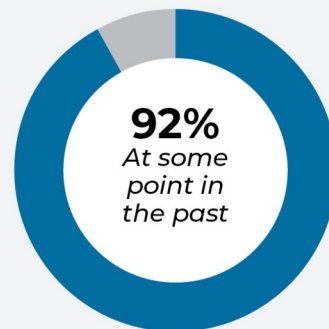As of Sep. 2023. Data shown is using current exchange rates.
Source: Statista Market Insights

statista

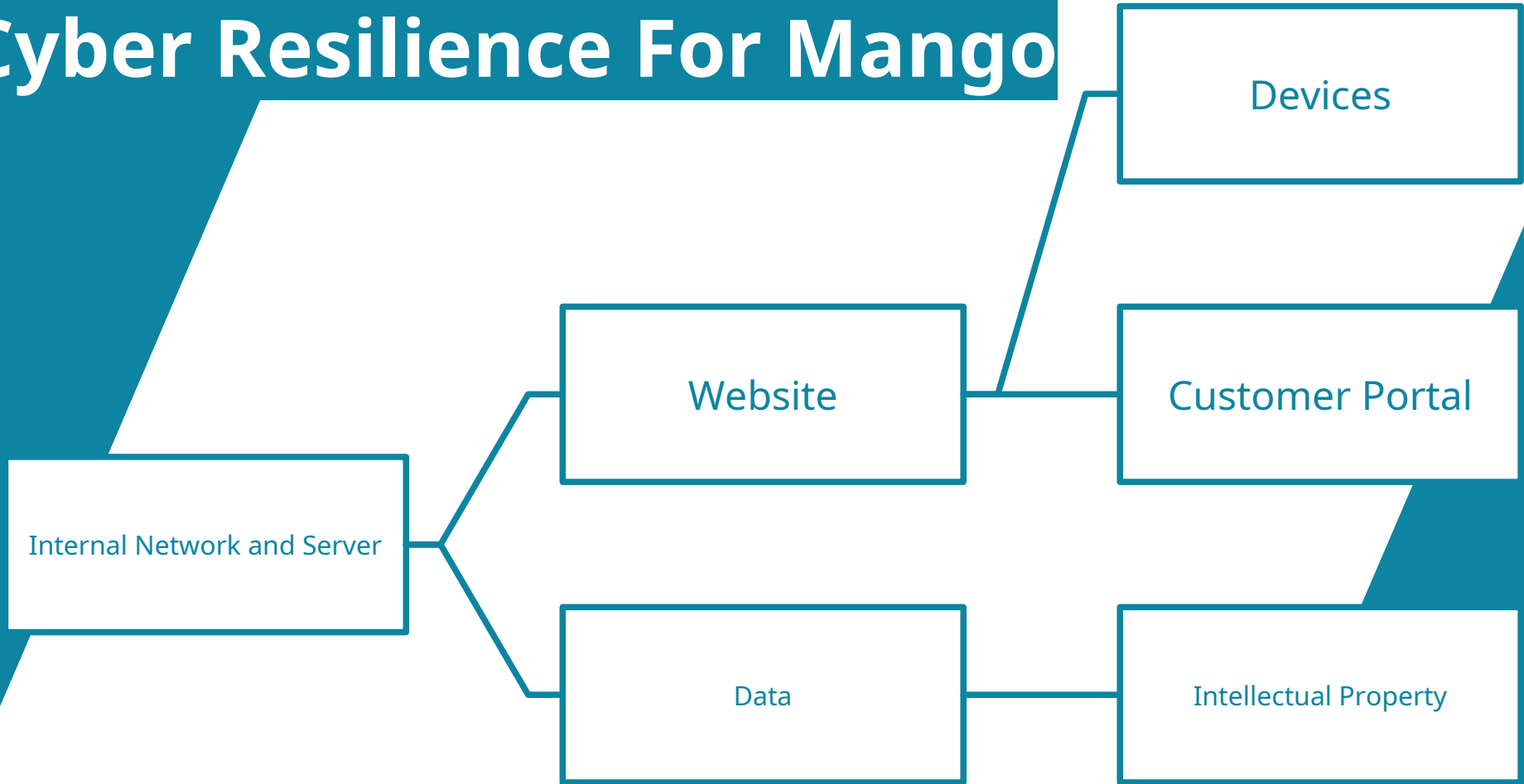## Most organizations have experienced a cyberattack
IT security decision-makers who have experienced a cyberattack

92% At some point in the past

82% Within the last 24 months

73% Within the last 12 months

Building A Strong Security Culture At Mango

- There is a unique opportunity for Mango to create a robust security culture from the ground up.

- With no existing security practices, Mango can establish a security-first mindset for our culture.

- Security is everyone's responsibility – not just IT. Every employee plays a critical role in the security of the company.

- Security should be ingrained into Mango's mission statement, core values, and policies.

- As an employee, training's should help you recognize threats, make informed decisions, and understand consequences of security lapses.

- Reward and empower employees to report suspicious activity and stay proactive on security.

Cyber Resilience For Mango

Internal Network and Server

- Website
  - Devices
  - Customer Portal
- Data
  - Intellectual Property

Cyber Resilience for Mango

- Mango will likely have a website, potentially with customer portals for accessing information, managing devices, and interacting with services. Protecting this entry point from common web-based attacks such as phishing, DDoS, and SQL injections is crucial.

- As a tech company, Mango will need a secure internal network to manage business operations and product development. Servers will likely support wearable device connectivity, data storage, and communication. Protecting these assets from ransomware, unauthorized access, and insider threats is critical to ensuring up-time and operational efficiency.

- Mango's operations will generate and store sensitive data, including product designs, schematics, and proprietary code. Securing this information with encryption, access controls, and regular backups will protect against theft and tampering.

Going Forward

- **Conduct a Formal Risk Analysis → Adopt a Cybersecurity Framework (such as NIST)**

- **Implement Security Policies and Procedures to Govern How Mango Handles Business Operations**

- **Implement Security Controls (i.e. Encryption, MFA, Firewalls, Access Controls, etc)**

- **Ongoing Risk Management**

  By taking a structured, proactive approach, Mango Wearable Solutions can establish a strong foundation for cyber resilience. Implementing these key steps will protect the company's critical assets, ensure compliance with regulations, and reduce the risk of operational disruption.