Trends in Smart Home Data Security and Privacy

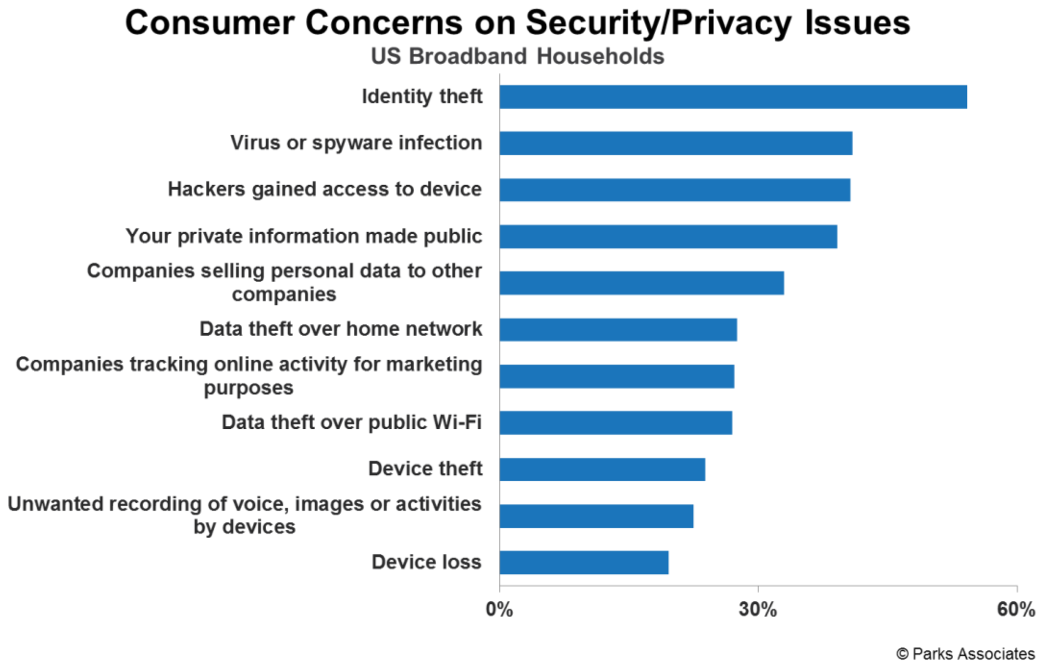
TABLE OF CONTENTS

By Denise Ernst, Vice President; Jennifer Kent, Senior Director; Weijun Lee, Research Partner; Chris O’Dell, Research Analyst; and Brad Russell, Research Director, Parks Associates

Synopsis

This report examines the challenges in securing the smart home and new opportunities for security solution providers. The report also assesses common and potential attacks in the connected landscape as new connected solutions, such as 5G technologies, are implemented. It profiles companies offering data security solutions for the connected home and product and service providers who are leading the way on securing the smart home.

Consumer Privacy Concerns



Publish Date: 4Q 19

Questions Addressed by this Report:

What are the typical incidences/challenges/solutions in protecting data security & privacy in smart homes?

What are the current and upcoming regulations related to data security and privacy in smart homes?

What should smart home manufacturers do to comply with regulations and meet consumer expectations?

How should data security solution providers educate smart home consumers about their responsibilities to keep their homes safe?

What new innovations are offered by best-in-class data security solution providers?

How do data/privacy issues and concerns impact the growth of the smart home market?

Contents

Research Objectives
Research Approach
Companies Interviewed or Researched

Executive Summary
Industry Insight
Data Security & Privacy Trends - User Experiences
Data Security & Privacy Trends - Technologies

© 2019 Parks Associates. All rights reserved.

Data Security & Privacy Trends – Marketing & Sales Channels
Connected Home Data Security and Privacy Ecosystem
Key Findings and Recommendations

Defining Data Security and Privacy
Data Security vs. Data Privacy
Trade-offs for Consumers
Classification of Data Security and Privacy Attacks
Targets and Objectives of Data Security/Privacy Attacks
Direct and Indirect Attacks
Privacy Vulnerabilities

Consumer Insights
Security/Privacy Concern and Problems (Q4/18)
Consumer Concerns on Security/Privacy Issues (Q4/18)
Actions Taken to Prevent Unauthorized Access to Devices (Q4/18)
Smart Home Devices: Purchase Inhibitors (Q4/18)
Appeal of Cybersecurity Services (Q4/18)
Appeal of Cybersecurity Services by Introduction Text (Q4/18)
Desirability of Cybersecurity Services (Q4/18)
Preferred Provider of Cybersecurity Services (Q4/18)

Data Breach Incidences and Vulnerabilities
Status of Data Breaches in Connected Homes
The 2016 Mirai Attack by Exploiting Default Username/Password
The 2017 Fish Tank Attack Showed Much Bigger Lateral Damages
The 2019 Nest Cam Hacking due to Credit Stuffing Attacks
Supporting Consumers: An Academic Study on Privacy Vulnerabilities in Smart Home
Turning Data Attacks into Physical Attacks
Data Privacy/Security Ecosystem Opportunities for Action

Regulatory Analysis on Data Security and Privacy
Legislations on Smart Home Data Security and Privacy
Leading Legislation: The EU General Data Protection Regulation (GDPR)
GDPR: The Smart Home Manufacturers Respond
Data Protection Laws in the US
Passed and Pending US Regulations and Standards
Federal Standards: Defining Cybersecurity and Privacy Risks for Organizations
Federal Standards: IoT Device Manufacturers
Pending Federal Legislation: IoT Device Manufacturers Selling to Government
State Legislation: California SB-327 Information Privacy: Connected Devices 2018
State Legislation: CCPA Affects Businesses Using Consumer Data
CCPA vs. GDPR - Summary
CCPA vs. GDPR - Details
Cybersecurity Impacts: Brand Perception and Fines

Business Models and Services
Business Models in Smart Home Data Security and Privacy
Interest in Security/Privacy Services (Q4/18)
A Taxonomy of Cybersecurity Solutions
B2C Business Model by Smart Home Service Provider
B2C Business Model by Broadband Service Provider
B2B Business Models
B2C and B2B Example: F-Secure

© 2019 Parks Associates. All rights reserved.

Business Models: B2B + B2B2C
CUJO AI Security Profile
CUJO AI: Unique Advantages
The Public/Private Partnership Model

Technology Opportunities

Technologies to Protect Data Security and Privacy in Smart Home
Tradeoff between Security and Convenience: TFA and MFA
Privacy Enhancing Technologies (PET)
Typical Privacy Enhancing Technologies
AI and ML Become Essential for Cybersecurity
Where and How to Apply AI/ML in Cybersecurity
Example: Cybersecurity AI Platform
Privacy by Design (PbD)
Impact of 5G to Smart Home Data Security and Privacy

Appendix

Glossary of Security Threats
Definition of Adversary/Threat Model
Capability Levels of Adversary & Threat Models

Attributes

Parks Associates
5080 Spectrum Drive
Suite 1000W
Addison, TX 75001

800.727.5711 toll free
972.490.1113 phone
972.490.1133 fax

parksassociates.com
sales@
parksassociates.com

Authored by Denise Ernst, Jennifer Kent, Weijun Lee, Chris O'Dell, and Brad Russell
Executive Editor: Tricia Parks
Published by Parks Associates

© November 2019 Parks Associates
Addison, Texas 75001

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher.

Printed in the United States of America.

Disclaimer
Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.