

Cyber Security in Smart Commercial Buildings 2017 to 2021

Published: Q2 2017

Cyber Security in Smart Buildings 2017



Synopsis

This report will help all stakeholders and investors in the Smart Buildings industry to identify trends and business opportunities.

© 2017 Meemoori
Research AB

Introduction

This Report is a Brand New 2017 Study, which makes an Objective Assessment of the Market for Cyber Security Software, Services & Hardware in Smart Commercial Buildings 2017 to 2021

Memoori presents a brand new report, building on our portfolio of building technology related research. This independent study makes an objective assessment of the current state of the market for **Cyber Security in the Smart Buildings sector**.

The report focuses on market sizing and opportunities for Smart Commercial buildings, providing a fresh market assessment based upon the latest information. Market sizing and market opportunities data is provided for four regions representing the main international markets of North America, Europe, Asia Pacific and The Rest of the World. Market sizing projections are broken down in terms of hardware, software and services.

See more at: <http://www.memoori.com/portfolio/cyber-security-in-smart-commercial-buildings-2017-to-2021>

Fig 8.2

A Layered Approach to Smart Building Cybersecurity



What This Report Will Tell You

Within its **160 pages** and **38 charts and tables**, the report sieves out ALL the key facts and draws conclusions, so you can understand exactly how Cyber Security is shaping the future of the Smart Building Industry.

There is a strong interrelationship between the BIOT market and the cyber security market for smart buildings. The increased proliferation of smart devices, combined with persistent concerns over cyber-risk and data privacy and an increased incidence of cyber attacks against smart buildings will help drive a significant increase in demand for new cyber security hardware, software and services in the market.

Based on extensive research into the dynamics of the market, as well as interviews with leading industry stakeholders, we estimate that global revenues for smart building cyber security will reach \$8.65 billion by 2020, up from an estimated \$ 4.26 billion in 2016, representing a healthy CAGR of over 15% over the forecast period.

Buildings control systems are increasingly being deployed along with embedded communications technology to provide critical services that allow a building to meet the functional and operational needs of building occupants. Smart buildings promise significant benefits to owners and operators in terms of efficiency, safety, comfort and functionality, **but these systems also carry potential costs, as without the right levels of protection, they can act as tempting targets for would-be hackers and or malicious insiders.**

This rise of the IoT offers up tangible business benefits and tantalizing new opportunities for innovative business approaches, but these need to be carefully weighed up against the potential risks of increased cyber security vulnerability. If the risks are not properly managed by stakeholders across the supply chain, we run the risk of undermining consumer confidence in the market.

In our regional analysis of market revenues for cyber security in smart commercial buildings, the North American market is the dominant global force, representing nearly half (47%) of global revenues in 2016 with just over \$2 Billion in annual revenues, rising at a CAGR of 13.8% to \$3.83 Billion by 2021.

Skills shortages exist globally, but are felt even more intensely in the European market, with 30% of companies unable to fill open cyber security positions, the U.S. is not far behind, with 27% having issues, while the Asian market fares better, with only 22% of roles unfilled. This skills shortage may well prove both dangerous and expensive. It leaves businesses vulnerable to attacks resulting in reputational damage and data loss.

Fig 1.3

Cybersecurity Threat Vectors for Smart Buildings

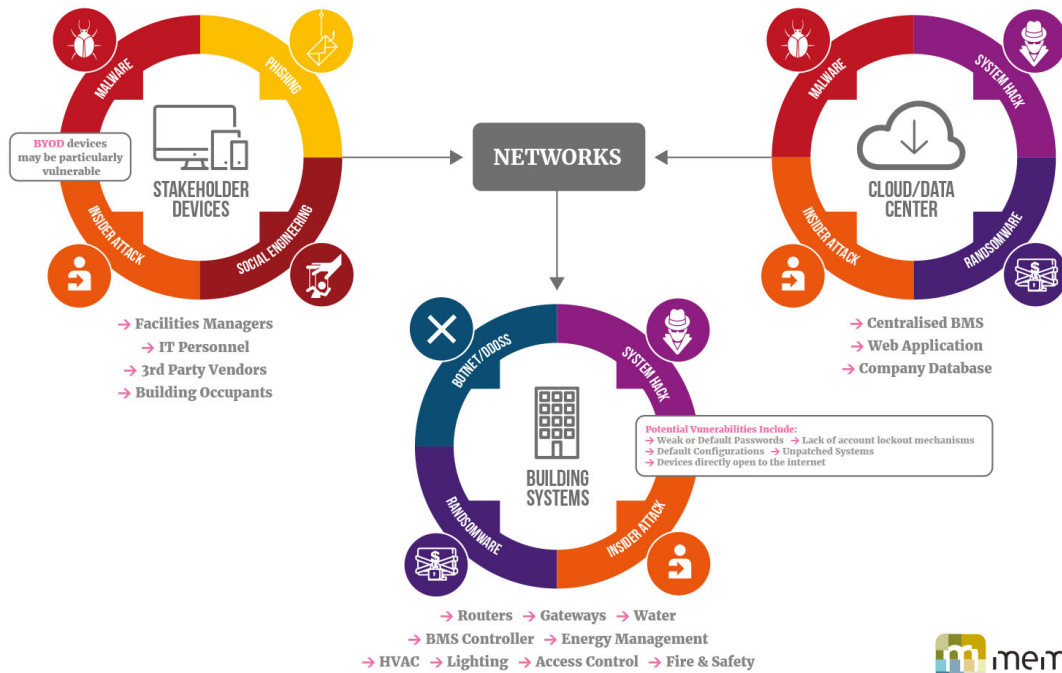


Table of Contents

Preface

Methodology

Definitions

Executive Summary

Part 1: The Current State of the Cyber Security in Smart Commercial Buildings

1. The Cyber Risk Threat Landscape

1.1 Cyber Security Threat Classification

1.2 The Cyber Attack Lifecycle

1.3 Cyber Security Threat Vectors

1.4 Cyber Security Attack Actors & Motivations

2. Cyber Security Risks for Smart Buildings

2.1 OT vs IT – Systems Convergence & Integration

2.2 The Impact of the IoT

2.3 Smart Buildings Risk Evaluation

2.4 Smart Building Costs & Impacts

2.5 Case Studies of Recent Attacks

Part 2: Market Sizing & Analysis

3. The Global Cyber Security for Smart Buildings Market - Sizing & Growth Projections

3.1 Hardware

3.2 Software

3.3 Services

4. Market Analysis by Region

4.1 Regional Comparisons

4.2 North America

4.3 Asia Pacific

4.4 Europe

Part 3: Vertical Market Analyses

5. Vertical Market Status & Opportunities

5.1 Vertical Market Comparisons

5.2 Offices

5.3 Retail

5.4 Banking & Financial Services

5.5 Hospitality

5.6 Government

5.7 Healthcare

Part 4: Drivers, Challenges & Best Practice

6. Market Drivers

6.1 Persistent Concerns Over the Risks of Cyber Security & Data Privacy

6.2 Rising Cyber Security Spending

6.3 Board Level Involvement in Cyber Security is Growing

6.4 Rising Incidence and Cost Impacts for Smart Buildings

6.5 IIoT Market Growth

6.6 Regulatory & Legislative Drivers

7. Market Challenges

- 7.1 Limited Market & Stakeholder Awareness of the Risks
- 7.2 Lack of Organizational Preparedness
- 7.3 The Cyber Security Skills Gap
- 7.4 Blurred Lines of Ownership, Control & Responsibility
- 7.5 Corporate Structure, Culture and Governance
- 7.6 Building Systems Limitations & Vulnerabilities
- 7.7 Limited IoT Device Functionality & Security concerns

8. Best Practice & Recommendations

- 8.1 Identify & Understand the Nature of the Threat
- 8.2 Prepare Governance, Strategies & Policies
- 8.3 Protect Networks & Systems
- 8.4 Monitoring & Detection
- 8.5 Incident Response & Recovery

Part 5: Cyber Security Standards & Regulations

9. Standards

- 9.1 Cyber Security Industry Standards
- 9.2 Building Control Related Standards

10. The Regulatory Environment

- 10.1 The State of Regulations for Cyber Security
- 10.2 Relevant National Regulations

Part 6: The Competitive Landscape & Market Dynamics

11. The Wider Cyber Security Vendor Landscape

- 11.1 The Wider Cyber Security Vendor Landscape
- 11.2 Cyber Security Products and Services

12. Smart Building Market Offerings and Vendor Strategies

- 12.1 Smart Building Market Offerings & Market Dynamics
- 12.2 Incumbent Building Controls Players
- 12.3 Emerging Players & Startups
- 12.4 Legal & Insurance Service Providers

13. Partnerships and Alliances

Part 7: The Investment Market

14. Cyber Security Deals Analysis

List of Charts & Figures

Fig 1.1 - Types of Cyber Attacks Experienced (2015-2016, 237 Benchmarked Companies)

Fig 1.2 – The Cyber Attack Life Cycle

Fig 1.3 - Cyber Security Threat Vectors for Smart Buildings

Fig 1.4 - Cyber Security Attack Motivations (Proportion of overall attacks)

Fig 2.1 - The Internet of Things in Smart Commercial Buildings

Fig 2.2 - Building Elements perceived to be at High Risk

Fig 2.3 - Awareness Levels of Cyber Security Issues for Building Automation Systems

Fig 2.4 - Shodan Results for Connected Devices - Selected Protocols April 2017

Fig 2.5 - Costs of Cybercrime (\$ million / Average Case)

Fig 3.1 - The Global Cyber Security for Smart Buildings Market - Sizing & Growth Projections

Fig 3.2 - Global Market for Cyber Security in Smart Commercial Buildings 2016 to 2021 (\$ Billion)

Fig 3.3 - Cyber Security in Smart Commercial Buildings - Revenues by Hardware, Software & Services 2016 to 2021 (\$ Billion)

Fig 4.1 - Cyber Security in Smart Commercial Buildings - Revenues by Region 2016 to 2021 (\$ Billion)

Fig 4.2 - Annualized Cost of Cyber Crime Incidents in Benchmarked Companies by Country (\$ Millions)

Fig 4.3 - Global Cyber Security Index

Fig 4.4 - Cyber Preparedness Rankings Comparison

Fig 4.5 - Cybercrime as a percentage of GDP

Fig 5.1 - Top 10 Industry Targets, % of Attacks 2016

Fig 5.2 - Password-Less Building Automation Systems that are Accessible via the Internet (% of Discovered Systems, August 2016)

Fig 5.3 - Security Rating by Industry (Selected Industries)

Fig 5.4 - Average Annualized Cost Impact of Cyber Crime by Industry Sector (Selected Industries, \$m)

Fig 6.1 - Leading challenges facing IoT implementations

Fig 6.2 - Cyber Security Spending Priorities (Oct 2016)

Fig 7.1 - Leading Shortages of Existing Skills in IT Organizations (Percentage of Respondents)

Fig 7.2 - Percentage of Companies unable to fill Open Cyber Security Positions in their Enterprises

Fig 8.1 - Cyber Security Best Practice

Fig 8.2 - A Layered Approach to Smart Building Cyber Security

Fig 14.1 - Cyber Security M&A Volume by Year 2012 to Q4 2016 (Number of Deals)

Fig 14.2 - Leading Cyber Security Startup Acquirers (Number of Acquisitions)

Fig 14.3 - Cyber Security Investment Deals 2012 to Q4 2016 (Total Number of Deals and Combined Value)

List of Tables

Table 1.1 - Cyber Security Attack Actors - Motivations & Objectives

Table 2.1 - Information Technology and Operational Technology Compared

Table 2.2 - Physical Impact Scenarios

Table 5.5 - Smart Building Cyber-Attack Risk Matrix by Vertical Market

Table 9.1 - Relevant Cyber Security Industry Standards

Table 9.2 - Building Control Related Standards

Table 10.1 - Relevant National Regulations

Table 13.1 - Partnerships & Alliances

How to Order

The report is priced at **\$1,500 USD** for a Single User License, and **ONLY \$1,750 USD** for an Enterprise License. It is delivered as an electronic PDF download, via email.

To order, or if you require further information please contact;

Jim McHale - jim@memoori.com / +46 76 190 3777

Alternatively you can order through our Website - <http://www.memoori.com/portfolio/cyber-security-in-smart-commercial-buildings-2017-to-2021>