Risk Assessment for IoT: A System Evaluation of the Smart Home and its Cybersecurity Imperative

By

Olivia Qing Gao

B. Math Computer Science/Bioinformatics options, 2004
University of Waterloo

Submitted to the Faculty in partial fulfillment of the requirements for the degree of Master of Science in Engineering and Management

At
Massachusetts Institute of Technology

June 2016

© 2016 Olivia Qing Gao. All Rights Reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Author: Signature redacted

System Design and Management Program
May 17, 2016

Certified by: Signature redacted

Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management
And Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Accepted by: Signature redacted

Patrick Hale
Director
System Design and Management Program
Risk Assessment for IoT: A System Evaluation of the Smart Home and its Cybersecurity Imperative

By

Olivia Qing Gao

Submitted to the System Design and Management Program on May 17, 2016 in Partial fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management.

Abstract

In the past two decades, the exponential growth of the modern Internet with the digitization of most human activities such as data gathering and storage have also fueled the growth of cybercrimes. In more recent years, the modern Internet is spreading into everyday life through the Internet of Things (IoT), which is further expanding the attack surface. Among all the IoT domains, the smart home, in particular, is poised to be one of the most exciting application areas of the IoT. However, behind the optimistic outlook, the shadow of an impending threat is also growing. Across the board, among the smart home device manufacturers, security is nearly non-existent or significantly downplayed. Consequently, the neglected, unresolved vulnerabilities in these devices widely expose their users and their family to cyberattacks.

This thesis aims to illuminate the dynamics in the smart home market and their implications for IoT as a whole. First, it will review the past evolution of the IoT and the smart home along with current trends in enabling technologies. Next, through detailed examinations of four dynamic factors - 1) macro pressures to innovate, 2) growing perils of cybercrimes, 3) vulnerabilities in the smart home, and 4) values at risk - the thesis seeks to elucidate the serious consequences of ignoring cybersecurity in the smart home system through causal loop diagramming. This thesis uses substantiated data from the past few years to justify its analyses.

The thesis concludes that the smart home is an essential innovation that can help solve many urgent challenges facing our time, and securing the smart home devices is a key step towards building a safer and more secure IoT future as well as a future for the current generation and many generations to come.

Thesis Supervisor: Stuart Madnick
Title: John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management
And Professor of Engineering Systems, School of Engineering
Acknowledgments

First, I would like to thank God for his love and discipline, and for this opportunity to further my study and become better equipped for tomorrow’s world. These past two and a half transformative years have tremendously expanded my horizon and worldview.

I have been fortunate to meet and receive invaluable inspiration, guidance, and mentorship from many people. First of all, this thesis would not have been possible without the patient instruction and constant support of my advisor Professor Stuart Madnick, who is not only an excellent academic advisor but also a thoughtful professional mentor. His wit, insight and feedback have enriched this last stretch of my educational experience at MIT immensely. I am glad to have met many cybersecurity experts through Professor Madnick’s research group. Allen Moulton, Jerold Grochow, Chris Zannetos, George Wrenn, Mohammad Jalali, Raphael Yahalom and Michael Siegel, thank you all so much for your incisive feedback which has led me to think one step ahead about what other questions I’ve been missing in my research. In particular, Mohammad told me about Professor Nelson Repenning’s paper that became the theoretical foundation to understand the dynamics in this thesis. Next, I owe the inspiration for the association of the smart home with sustainability to Professor John Sterman’s class, “Strategies for Sustainable Business,” which I took in the first half semester of Spring 2016. Some of the data used in this thesis also came from lecture notes/articles drawn freely from the class. Other thought leaders that have shaped the direction of this thesis are Professor Michael Cusumano, Professor John Carroll, and Senior Lecturer Michael Davies. Furthermore, I’d like to thank Colonel Bill Young for sharing his knowledge about security case studies. I’d also like to thank Sloan Fellow Natasha Nelson for sharing her study on innovation and cybersecurity, including her survey data. Moreover, I am grateful to Principal Research Scientist Dr. Donna Rose for giving an hour of her time to chat about system engineering methodologies in the very early stage of this thesis.

I’d like to thank the System Design and Management program (SDM) for believing in me and allowing me the opportunity to learn. Special thanks go to the Director of SDM, Pat Hale, whose kindness and encouragement were essential to my positive experience in the SDM program. Additionally, I would like to thank Joan Rubin and Bill Foley for their support throughout my time in the SDM program.

I am thankful to friends who have been praying for me during difficult times.

My utmost sincere gratitude goes to my closest family, particularly my mother, for teaching me the true meaning of love. This important lesson gave me the strength and wisdom to make choices in life as well as the sense of purpose to carry on. I dedicate this thesis to her.
Table of Contents

Abstract ................................................................................................................................. 3
Acknowledgments .................................................................................................................. 5
Table of Contents ................................................................................................................ 7
List of Figures ....................................................................................................................... 9
Glossary ................................................................................................................................. 10

1 Introduction .......................................................................................................................... 13
  1.1 Context .......................................................................................................................... 13
  1.2 Personal Motivation ...................................................................................................... 14
  1.3 Objectives ...................................................................................................................... 15
    1.3.1 Problem Statement ............................................................................................... 15
    1.3.2 Clarifications of Terminologies, Scope & Limitations ........................................ 16
  1.4 Methods.......................................................................................................................... 18
    1.4.1 Systems Theory ..................................................................................................... 18
    1.4.2 Causal Loop Diagram ........................................................................................ 19
  1.5 Thesis Structure ............................................................................................................. 22

2 IoT and Smart Home Overview .......................................................................................... 24
  2.1 IoT Evolution ................................................................................................................ 24
  2.2 Systems Theory Applied to IoT ................................................................................... 25
  2.3 Smart Home Evolution .................................................................................................. 25
  2.4 Technology Enablers ..................................................................................................... 26

3 Macro Pressures to Innovate ............................................................................................. 30
  3.1 Societal/Consumer Needs ............................................................................................ 30
    3.1.1 Sustainability Need .............................................................................................. 30
    3.1.2 Social Need .......................................................................................................... 34
    3.1.3 Economic Need ..................................................................................................... 35
    3.1.4 Objectives of the Smart Home ............................................................................. 36
  3.2 Business Pressures ........................................................................................................ 37
    3.2.1 Technology Incumbents Quandary ....................................................................... 37
    3.2.2 Global Competition ............................................................................................. 38
    3.2.3 Rising Consumer Demand ................................................................................ 39
  3.3 Causal Loop Diagram .................................................................................................. 40

4 Growing Peril of Cybercrimes ............................................................................................ 42
  4.1 Types of Cyberattacks ................................................................................................. 42
  4.2 Attacker Profiles .......................................................................................................... 45
  4.3 Current Trends .............................................................................................................. 46
    4.3.1 Thriving Underground Ecosystem ...................................................................... 46
List of Figures

Figure 1-1: Three Types of Systems (Leveson, 2012) .................................................................. 19
Figure 1-2: Innovation Process (Repenning, 1999) .................................................................. 20
Figure 1-3: Expert Reinforcement Process (Repenning, 1999) .................................................. 21
Figure 2-1: Improvements of Various Technologies Over the Past Few Decades (Brynjolfsson & McAfee, 2014) ........................................................................................................................ 27
Figure 3-1: Reasons that US Internet Users Would be Interested in Purchasing Smart Home Devices (eMarketer, 2016) ........................................................................................................... 32
Figure 3-2: How Environment, Society and Economy Relate to Each Other (MIT Sloan Class "Strategies for Sustainable Business") .......................................................................................... 36
Figure 3-3: Effects of Customer Expectations on Companies (eMarketer, 2015) .............. 39
Figure 3-4: Smart Home Pressure to Innovate Causal Loop Diagram ....................................... 40
Figure 4-1: Types of Cyber Attackers (Han & Dongre, 2014) ................................................. 46
Figure 4-2: Compromise vs. Discover Efficiency (Verizon, 2015) ............................................. 48
Figure 4-3: The Impact of the Escalation in Cybercrimes on the Smart Home ...................... 52
Figure 5-1: Existing Expectations for Device Lifecycle (OECD, 2013) ........................................ 59
Figure 5-2: Autho Survey Results of IoT Developers ............................................................... 62
Figure 5-3: Number of Smart Devices in a Household of Four (OECD, 2013) ......................... 64
Figure 5-4: Vulnerabilities of the Smart Home Causal Loop Diagram ..................................... 67
Figure 6-1: Number of Startups and Amount of Venture Invested for Each IoT Category (Venture Scanner, 2015) ................................................................................................................................. 70
Figure 6-2: Final Causal Loop Diagram ..................................................................................... 80
Glossary

**Attack vector**: a path or means by which a hacker can gain access to a computer or network in order to cause a damaging outcome.

**Botnet**: an array of compromised private computers infected with malware controlled as a group to send spam messages or carry out other malicious tasks such as the distributed denial-of-service (DDoS) without the owner ever knowing.

**BAS**: building automation systems.

**Causal loop diagram**: a simple map of a system with all its constituent components and their interactions.

**Computer virus**: a piece of software that can self-replicate and move into other computer programs, data files, and even the hard drive to cause widespread harm.

**Cyberattack**: the act of committing cybercrimes.

**Cybercrime**: an offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks.

**Cyber-Physical System**: an integration of computation, networking, and physical processes.

**Cybersecurity**: the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

**Denial-of-service (DoS)**: a type of cyberattack that intends to bring an online service down by overwhelming the system limit with massive traffic, which can come from many locations and sources.

**Distributed Denial-of-Service (DDoS)**: a type of DoS where multiple systems infected with a Trojan are used to conduct DoS attacks on a single system.

**DOT**: Department of Transportation.

**FBI**: Federal Bureau of Investigation.

**Fullz**: full information package.

**Malware**: malicious software as the software's creation intent is malicious.
Net Zero Energy Home: a home with zero net energy consumption because the total amount of energy used by the home per year is equivalent to the amount of renewable energy created by the home itself.


Internet of Things (IoT): the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Ransomware: a type of malware that extorts a payment from its victims by locking their systems and data.

Reconnaissance: a process in which intruders engage with the targeted system to get information about vulnerabilities such as a list of possible attack vectors (a path or means by which a hacker can gain access to a computer or network to cause a damaging outcome) that can be exploited later for further attacks.

SMAC: social, mobility, analytics and cloud.

Smart home: a home equipped with lighting, heating and electronic devices that can be controlled remotely by phone or computer.

Social Engineering: any act that influences a person to take an action that may or may not be in their best interest.

System: an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements.

System dynamics (SD): an approach to understanding the nonlinear behavior of complex systems over time using stocks, flows, internal feedback loops, and time delays.

System of systems (SoS): systems-of-interest whose system elements are themselves systems; typically, these entail large-scale inter-disciplinary problems involving multiple, heterogeneous, distributed systems. These interoperating collections of component systems usually produce results unachievable by the individual system alone.

System thinking: centered in context, interfaces and emergent behaviors – the interstitial elements around and within the system; the “whole” rather than the decomposed element.
**Time to market:** length of time taken in product development process from product idea to the finished product. It is a critical component of time-based competition.

**Thingbot:** Internet-connect embedded system that is infected with malware and coopted into part of a botnet.

**Watering hole:** an attack that uses a combination of social engineering with malware that targets a particular group rather than individuals.

"**Zero-day** exploit:** a security flaw in popular software previously unknown to their vendors, and therefore, unpatched.
1 Introduction

"We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

– IBM Chairwomen Ginni Rometty

1.1 Context

Over the last few years, the rapidly changing technology landscape has ushered in a new era of the information revolution, namely, the Internet of Things (IoT) revolution. However, this advancement along with its promised benefits in improving the quality of life and bringing about vast economic opportunities have also introduced potential unforetold new risks; chief among them all are new potential challenges for security breaches.

In a 2015 episode of the high-tech American drama TV series Scorpion, a “smart” building infected with a deadly virus has trapped everybody inside including children and induced a series of safety hazards that almost end in casualties. Fortunately, the world today has not yet become as dramatic as depicted in this scary TV show, but cybersecurity breaches are already looming large in recent years with unprecedented consequences.

In 2015, Inga Beale, the CEO of the British insurance company Lloyd’s, estimated that the insurance industry charged $2.5 billion globally in premiums on hacker coverage that year (a 25% increase over the previous year), and cyberattacks cost businesses collectively as much as $400 billion each year. The cost to the US businesses alone is near $100 billion per year. (Gandel, 2015) Another study conducted by IBM in the same year concluded that companies with at least 1,000 employees saw an average total cost of a data breach at about $15.4 million per company – a 19% increase from its 2014 study (Morgan, 2015). These numbers only include the financial cost and does not take into account the less tangible aspect such as privacy violation of customer data, damage to companies’ brands and losses in customers’ trust. Many large companies such as Home Depot, JPMorgan Chase, eBay, Sony and Target have all fallen victim to cyber breaches, and each instance resulted in financial losses of millions of dollars or personal information compromises affecting millions of people and sometimes both. In 2015, the largest financial digital robbery involved at least 100 banks in 30 countries and stole a whopping $1 billion (Snider & Whitehouse, 2015). That same year, the US government Office of Personnel Management was hacked, exposing background
check information on nearly every federal employee, about 4.2 million workers (Rein & Peterson, 2015).

With the recent advancement of the IoT evolution, the threat landscape is also rapidly evolving with some high-profile breaches occurring in recent years. In 2015, a group of hackers managed to take control of a Jeep Cherokee remotely and cut the car's brakes and turn off its engine while it was still on the highway. This same hack would have worked in any of the earlier 2013 to 2015 Chryslers and the Tesla Model S. The hack resulted in millions of recalls for Chrysler while the Tesla patched all its Model S vehicles over the air. (Luckerson, 2015) In a 2016 report, a joint public announcement from the FBI (Federal Bureau of Investigation), DOT (Department of Transportation) and NHTSA (National Highway Traffic Safety Administration) "lists wireless components of modern vehicles that can be vulnerable" and the methods to attack them. (The Trucker News Services, 2016) Apart from connected cars, violations in other connected devices can also lead to fatality; for example, a hacked insulin pump can be maliciously activated to cause patient death. Hence, in 2007, former Vice President Dick Cheney had to disable the Internet connectivity in his pacemaker (Peterson, 2013). In fact, having weak or no cybersecurity measures is not an isolated event affecting only a limited number of devices but rather an industry phenomenon. In 2014, an investigation by the US Department of Homeland Security on the security of medical devices concluded that 300 devices from 40 different companies had hard-coded passwords (Cylance, 2015). And Symantec said in 2014 about 20% of health IoT devices sent logins, passwords and personal information in clear text (Klostermann, 2015). The rapid growth in digitization as well as the widespread security issues in IoT products would trigger the cost of data breaches to upsurge four times the estimated amount in 2015 to $2.1 trillion globally by 2019, according to Juniper Research (Juniper Research, 2015).

As Eugene Kaspersky, the founder of Kaspersky Lab, one of the world's most prominent anti-virus companies, famously said, "You can call it Internet of things; I call it Internet of threats." (Weissman, 2015)

### 1.2 Personal Motivation

Besides the reason that cybersecurity has important effects on safety, data security and privacy, as well as massive economic consequences which caused it to become the main barrier to technological adoption, one of the key causes that led me to this topic are personal. During my college years, a time when there was an explosive growth of malware, one of my biggest frustrations was the influx of spam that inundated my inbox almost every day even with the spam filter in place. At one point, I naively clicked on a link in a phishing email, and only learned much later that the link contained a virus which took control of my computer and caused it to
shut itself down at seemingly random times. I eventually had to abandon that disabled computer, a bulky Dell laptop and the first computer I had ever owned.

As I become a more sophisticated Internet user, this distressing experience has always been at the back of my memory. Because I knew first-hand the pain of data loss and privacy violation, I feel this is a topic I’d like to learn more about and make a contribution to.

1.3 Objectives

"There is nothing more important than a good, safe, secure home."

- Rosalynn Carter

1.3.1 Problem Statement

Throughout the time this thesis was written, there have been tens of thousands of published articles, research papers, and news reports on the subject of cybersecurity, IoT and the smart home (an application/subdomain of IoT). Most literature focuses on prioritization based on economic impacts of different subdomains of IoT or specific technical aspects of IoT, smart homes and cybersecurity individually. None of the reports (that I found or have access to) during the time frame of this research was conducted considers IoT as a system of systems, and the smart home a system of systems within the system of IoT and how cybersecurity in the smart home will impact the entire IoT system’s success. A “Systems-of-Systems” (SoS) is created to address large-scale, inter-disciplinary problems by composing multiple heterogeneous distributed systems because these problems are infeasible to be solved by individual systems alone (International Council on Systems Engineering (INCOSE), 2011). The smart home is a SoS because it consists of multiple heterogeneous systems that are themselves an integral part of other systems. For instance, a smart home energy system is on its own a complex system and an integral part of the smart grid system, and likewise, the smart home healthcare system is part of the smart hospital system. The IoT is a system of systems also because it comprises multiple systems such as the smart enterprise and the smart home. Additionally, there is no report that links the importance of smart homes with the key challenges facing our time. In other words, the smart home is just one out of many IoT application areas and currently does not attract the attention it deserves except from consumers and innovators. This suggests that there is an opportunity to apply system thinking to provide a richer picture of why the smart home market is a key IoT domain. Moreover, cybersecurity is just one critical success factor among many factors such as safety, reliability, user experience and costs, but currently, as evidenced by many breach cases, it is not a top priority on the agenda of its key stakeholder. This thesis seeks to understand the sources of vulnerabilities as well as the
critical consequences of neglecting the current cybersecurity vulnerabilities in the smart home.

By applying system thinking to analyze the complex cyber-physical system surrounding the smart home, the main research objectives of this thesis are to:

**O1:** Explore the rationales behind the emerging trend of the smart home to establish the importance of this market, and to clarify the high-level goals for the smart home.

**O2:** Understand the criticality of the cybersecurity requirement, various dynamic forces at play and the consequences of not meeting it in the smart home.

Furthermore, although there are growing concerns about cybersecurity as a significant barrier to IoT growth in general, these opinions have not yet pushed the industry to work together towards a resolution. Through the application of some rigorous system methodologies, this thesis aims to provide data to technology experts, law and policy makers, company executives, investors, researchers and consumers in the hope of bringing their attention to this topic for further investigation and debate, especially further applications of system methodologies on this topic.

### 1.3.2 Clarifications of Terminologies, Scope & Limitations

A “thing” in the IoT taxonomy is called “smart” when sensors imbue it with the ability to connect to the Internet, and this connection allows them to talk with each other. By this definition, the majority of modern households are already “smart” because many of them have broadband connections and uses devices such as smartphones, smart TVs, laptops, etc. In the Oxford dictionary, the “smart home” has a stricter meaning, defined as a home with lighting, heating, and electronic devices; each can be controlled remotely by a phone or a computer. In this thesis, the “smart home” refers to homes with a growing collection of Internet-connected products in combination with complementary services that are brought into the home and provide the users with the ability to monitor/manage their home energy/resource/security utilization from afar as long as they have an Internet connection. The smart home is sometimes also called the connected home. In this thesis, smart home and connected home are assumed to have the same meaning.

Cybersecurity has different meanings for different stakeholders. On the one hand, cybersecurity from governments’ perspective means national security as they may need to access and intercept communications and gather intelligence for the purpose of law enforcement and thwarting terrorist attacks. On the other hand, for the private sectors and consumers, cybersecurity means protection from illegitimate access, deliberate attack, accidental compromise and unauthorized use of their personal and intellectual properties as well as other private information through
security measures such as encryption. There seems to be a conflict of interest between these two views, but the purpose of this thesis is not to take a side in either these views nor is it to explore possible win-win solutions. Rather, this thesis focuses on discussing the interesting dynamic forces surrounding the cybersecurity for the smart home and how they may play out in the broad landscape. For a consistent definition, this study takes on the meaning of cybersecurity from the perspective of the consumers specifically for IoT in the context of the smart homes. Furthermore, there are many references to home security systems online, specifying a sub-category of smart home products that allow users to monitor homes remotely and detect intrusions. The cybersecurity explored in this thesis, not to be confused with home security systems, concerns the security risks for the smart home products as a whole.

There are many other critical success factors for IoT such as reliability, safety, usability, interoperability, affordability, and the underlining technical issues. For example, one of such technical issue is underscored in a study sponsored by the National Institute of Standards and Technology (NIST), which expresses concerns that the lack of precise and verifiable timing systems in computers and networks may hinder the development of the IoT because IoT systems depend on accurate synchronization across networks. The lead author Weiss says, “Imagine writing a letter to your friend saying it is now 2:30 p.m., and then sending it by snail mail so he can synchronize his watch with yours... That’s the equivalent of how accurate the timing of messages is in computers and systems right now. The transfer delay must be accounted for to do the things that are expected of the IoT.” The publication further calls for interdisciplinary research to design and implement the correctness of timing into systems. (NIST, 2015) This factor and many other factors are not the focus of this thesis because they are often dependencies on how systems should work properly. By comparison, cybersecurity is a relatively new threat because many objects in the home environment were previously unconnected and thus secure and because it is often off the radar for device manufacturers; therefore, stakeholders are less prepared to deal with cyber breaches in the new “smart home” environment.

This thesis focuses on providing, organizing data and connecting dots on the key dynamic factors surrounding the topic, thus illuminating the cybersecurity implications for the smart home as well as the entire IoT system. It does not attempt to recommend solutions on how to implement cybersecurity in the smart home.

Some scientists have raised a concern about the use of radiofrequency fields (RF), the enabling technology for all mobiles phones, Wi-Fi, and IoT, on public health. However, to date, there is no consistent scientific evidence for a causal relationship of adverse health effects from exposure to RF. The World Health Organization (WHO) is currently running an assessment of all previous studies on RF, and this assessment is due to be completed in 2016. (WHO, 2014) Possible impacts of IoT on
public health are beyond the scope of this thesis, which is based on the current knowledge on the utilization of RF.

Although this paper tries to be comprehensive, it does not attempt to account for all factors that may determine the impact of cybersecurity in the smart home and how that impact propagates to the other IoT domains. For example, one such factor is the social, technical environments of different geographic areas in the world. An interesting event happened recently in April this year namely the Panama papers, a leak of 11.5 million confidential documents with detailed information about many world leaders' hidden assets in offshore companies through a Panamanian law firm Mossack Fonseca (Temperton & Burgess, 2016). As can be seen, besides being an excellent example of awful cybersecurity, this event shows that the responses in various countries to this fallout are quite different. Similarly, the impact of smart home breaches on other IoT domains not only depends on the size and severity of breach but also the social, technical context where IoT businesses operate. The latter is beyond the scope of this thesis; the focus of this thesis is simply on explaining that cyber breaches in the smart home are going to be having an effect on other IoT businesses.

Finally, the analysis is not intended to be exhaustive; instead, it's meant to serve as an exemplary framework for thinking. Facts were gathered from various sources to achieve the author's objectives. But due to constraints of time and the absence of quantitative data, 1) modeling is limited to causal loop diagrams, not a complete stock-and-flow system dynamics model, and 2) it's possible there are missing values in this study.

1.4 Methods

Basic methods used in this thesis are objective formation, then extensive qualitative research and review of existing information from the press, existing research reports, books previously read, companies' websites, and other public resources on the topic. Then a causal loop diagram, that elucidates the dynamic causal relationships among the key driving factors, summarizes each chapter.

1.4.1 Systems Theory

In his book originally published in 1975, Gerald Weinberg proposed three types of systems (Figure 1-1):

1. Organized Simplicity (machines) systems that can be physically decomposed into subcomponents or subsystems for analysis because interactions between components are known and predictable.
2. **Unorganized Complexity (aggregates)** systems that exhibit a high degree of complexity and randomness and are best suited to be analyzed statistically.

3. **Organized Complexity (systems)** systems that are too structured to be analyzed by statistics and too complex to be understood with physical decomposition. (Weinberg, 2011)

![Figure 1-1: Three Types of Systems (Leveson, 2012)](image)

Systems theory was developed specifically for the third category of systems. Systems theory states that systems should be taken as a whole, not separately. In her 2012 book, Professor Nancy Leveson explained the pivotal reason that physical decomposition or so-called “analytic reduction” is insufficient to address complexity in modern systems. The reason is that systems do not operate independently and have emergent behaviors as components and events of systems are subject to feedback loops and other nonlinear interactions. Many modern engineering systems are frequently complex but structured software; therefore, they are in the third category of systems, and are well within the domain of systems theory. (Leveson, 2012)

### 1.4.2 Causal Loop Diagram

#### 1.4.2.1 Description

A causal loop diagram is a visualization of how different variables in a system are interdependent. It consists of a set of variables and arrowheads. Arrowheads denote
the causal direction as well as whether it's a positive relationship (an arrowhead marked positive indicates that the two connected variables change in the same direction) or a negative one (an arrowhead marked negative indicates that the two linked variables change in opposite directions). A closed circle in a causal loop diagram should be either labeled as a reinforcing loop or a balancing loop. A reinforcing loop is where an action produces a result that strengthens the same action. A balancing loop is where an action produces a result that weakens the need for the same action. (Sterman, 2000)

1.4.2.2 Base Model

This thesis is built upon the two causal loop constructs in Professor Nelson Repenning's 1999 paper as shown in Figure 1-2 and 1-3 respectively.

![Causal Loop Diagram](image)

Figure 1-2: Innovation Process (Repenning, 1999)

**R1 – Reinforcement** is a reinforcing loop where an increase in the level of results leads to more commitment to the innovation, which, in turn, increases the effort allocated to the innovation which then causes further results.

**R2 – Diffusion** is a reinforcing loop where more results beget positive observation of effort-and-result linkage by others, then, in turn, beget increased commitment to
the innovation and then, more effort is allocated to the innovation, which then leads to more results.

_B1 - Normative Pressure_ is a balancing loop where managers' goal for commitment is compared with the actual commitment to the innovation to assess the commitment gap which leads to management's normative pressure to close the gap.

Overall, Figure 1-2 describes the evolution of an innovation effort.

Figures 1-3 explains the scenario where there are two implementation areas, and experts' resources are limited so if the experts believe that the innovation in one area works out better as indicated by better results, they will invest more time and energy in that area (Repenning, 1999).

![Figure 1-3: Expert Reinforcement Process (Repenning, 1999)](image)

1.4.2.3 Model Assumptions

This thesis makes the following assumptions:

_A1_: a successful innovation in the smart home space is attainable given the speed of development of technologies.

_A2_: IoT is the best available technology to tackle some key challenges facing our time such as climate change. These challenges will be discussed in detail in Chapter 3. In all appearance, this seems to be the case but there might exist technologies that
the author is unaware of that are comparatively effective.

A3: the perception of the value of innovation is not only influenced by results but also influenced by industry interests and support from experts.

A4: the pressure to solve the key challenges facing our time such as climate change do not change dramatically during the IoT innovation.

A5: to ensure the causal loop model is manageable, the system boundary is set to be the IoT industry only. Other potential innovation areas are excluded from consideration in this thesis. (Repenning, 1999)

Finally, the causal loop diagrams at the end of each chapter are created to achieve the objectives stated in Section 1.3.1 for illustration purpose only, and hence do not include all factors discussed in the chapters but rather only aggregates or the most interesting ones.

1.5 Thesis Structure

This thesis is structured as follows.

Chapter 2 - IoT and the Smart Home Overview

This chapter presents the evolutionary stories and key technology components that form the foundation of IoT and the smart home.

Chapter 3 - Macro Pressure to Innovate

This chapter analyzes some of the macro pressures facing our time and their relationship to the smart home innovation.

Chapter 4 - Growing Peril of Cybercrimes

This chapter describes various attack methods and characterizes different attacker profiles.

Chapter 5 - Vulnerabilities of the Smart Home

This chapter discusses a selection of recent breach cases in the smart home and examines in depth the sources of the smart home vulnerabilities.

Chapter 6 - Values at Risk

This chapter focuses on the incentives that could attract real-life cyberattacks and the values at risk if breaches do occur.
Chapter 7 – A Selection of Promising Technology Advancements

This chapter describes four key promising recent developments in security technology.

Chapter 8 - Conclusion

This chapter summarizes key findings and confirms the objectives stated in the Introduction Chapter are achieved. It also provides directions for potential future research.

At the end of each chapter, the causal loop diagram developed in the previous chapter is extended with the addition of new information from the main discussions in the current chapter.
2 IoT and Smart Home Overview

"I've always been more interested in the future than in the past."

- Grace Hopper

2.1 IoT Evolution

"The real problem is not whether machines think but whether men do."

- B. F. Skinner

Already in 1926, Nikola Tesla described beautifully his vision for the future in an interview with Collier magazine, "When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole." In 1991, Mark Weiser, the father of ubiquitous computing, said in his prominent paper "The Computer for the 21st Century" that "the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." Eight years later, the term IoT was coined by British entrepreneur Kevin Ashton, a co-founder of MIT's Auto-ID centers, in a presentation he made at Proctor & Gamble, where he made the first connection between the new idea of Radio-frequency Identification (RFID) in P&G's supply chain and the emerging Internet. (Postscapes) Since then, the Auto-ID centers were renamed Auto-ID Labs and have become the leading global IoT research network comprising seven of the world's most renowned academic labs (Auto-ID Labs).

So-called “Things” in IoT are everyday objects that were once analog or mechanical in nature such as devices, cars, buildings, etc., become digital through the integration of embedded electronics, software, and Internet connectivity. They can collect information from their environment and exchange data with each other and cloud hosts as well as analytical engines on the Internet. Because of their capability to make sense of and leverage their environment, these objects are often called "smart" and can enable context-aware automation without human operation in nearly every field. (Wikipedia - Internet of Things) Interestingly, the method of monitoring machine performance in real-time has already been widely used by engineers in Original Equipment Manufacturers (OEMs) for a long time and was once called telematics and mobile resource management (Rezendes & Stephenson, 2013). Moreover, the Internet of Everything (IoE) is a superset of IoT. IoE is the all-encompassing word that captures an end-to-end ecosystem of people, things, data and processes, including all connectivity use-cases. (Jaiswal, 2015)
2.2 Systems Theory Applied to IoT

"94% of problems in business are systems driven and only 6% are people driven."

- W. Edwards Deming

By the definitions in Section 1.4.1 on systems theory, both the IoT and the smart home are systems with organized complexity thus are subject to the rule of systems theory. Currently, the most commonly used decomposition method in the world today for the IoT unfortunately does not use system thinking and is a physical decomposition where the IoT is classified by locations or settings, meaning within the settings of the physical environments in which IoT systems can be installed. The reasons for location-based IoT categorization are that 1) it facilitates the understanding of the process in which different IoT systems, the interconnections among these systems and dependent IT systems and databases create value for all stakeholders, and 2) IoT in different contexts will have different operational and technical requirements. Figure 2-1 illustrates one such generalized classification of IoT.

![Figure 2-1: Location-based Decomposition of IoT](image)

This thesis assumes this taxonomy, but further explains why considering each subcategory of the IoT and the smart home separately using physical decomposition is insufficient.

2.3 Smart Home Evolution

"I long ... to be at home wherever I find myself."

- Maya Angelou
The idea of the smart home started with the idea of the automated home, and can be dated back to 1950. A study in then-popular magazine *Popular Mechanics* featured a manor designed by mechanical engineer Emil Mathias that had most of the everyday tasks automated with the push of a button. (Sung, 2015) In 1969, Honeywell 316 tried to sell a Kitchen Computer for $10,000 to no avail. Not even a single unit was sold. (Hernandez, 2012) In 1970, Xio was the first home automation system that enabled home appliances to talk to each other through wired power line. 1982 is the year when the first Internet-connected appliance, a Coke machine at Carnegie Mellon University, came into existence. The machine could report stock details and soda status as well as show a graphical display of coke temperatures. (The Carnegie Mellon University Computer Science Department) Nest learning thermostat was the first commercial smart home product available to the public in 2011. In 2013, Microsoft launched “Lab of Things,” an open source platform that enables experimental research of innovative smart devices in homes (Microsoft Research). As of 2016, a company called “SmartThings” sold about 120,000 hubs that allow consumers to link nearly every connected gadget at home, whereas the Wink smart hub was sold to nearly one million consumers (Herceg, 2016).

While many technology companies took a product or platform approach, some other companies took a more integral path. In 2014, Honda unveiled a net zero energy research “smart home” at the University of California Davis campus to demonstrate that zero-carbon living is fully achievable with existing technologies. The house uses solar energy to heat and cool and generates enough power to take on the daily charge of a Honda electrical car and even contribute energy back to the local utility. A multitude of advanced sensors in the house allows it to track all its electricity and water usage, and Honda made all the data freely available to the public through open source. (Lavars, 2014) Later that same year, Velux America, a world leader in roof windows and skylights, built a prototype sustainable connected home in the St. Louis suburb of Webster Groves, MO, named Active House USA. The Active House USA was developed using the leading sustainability and high-performance building practices from around the world. (Hower, 2014)

### 2.4 Technology Enablers

“Computer is not about computers any more. It is about living.”

– Nicholas Negroponte

In recent years, the concept of the IoT has already been gaining widespread momentum due to a range of rapid advancements in wireless protocols, sensors, processors, data analytics, and cloud technologies. Mainly, the IoT is enabled by the following five technology trends.
The Rule of Exponential Growth: In 1965, Gordon Moore, the co-founder of Intel, made a prediction, which states that transistors on Integrated Circuits doubles approximately every two years. This prediction also known as Moore’s Law, became the golden rule for the electronics industry. Many critical building blocks of computing such as microchip density, processing speed, storage capacity, energy efficiency, download speed, and so on, have been following Moore’s Law and improving at exponential rates for a long time (Figure 2-1). With the IoT, objects incorporating digital components that give them Internet connectivity become subject to the exponential development trajectories of Moore’s Law. Consequently, the cost of bandwidth, hardware, sensors, chipset and processing speed are all falling rapidly, and the falling costs are what makes the IoT economically feasible to pervade everyday lives. (Brynjolfsson & McAfee, 2014)

![Figure 2-1: Improvements of Various Technologies Over the Past Few Decades (Brynjolfsson & McAfee, 2014)](image)

IPv6: IPv4 supports 32-bit address, which translates to about 4.3 billion addresses, less than the 7.4 billion people on earth, and has become nearly depleted by all the connected devices globally. In contrast, IPv6 supports 128-bit addressing, translating to approximately $3.4 \times 10^{38}$ addresses for every person in the world, which is virtually unlimited and provide more than enough IP addresses per person. This large address
space made the idea of any embedded object or device in the world to have a unique IP address on the Internet a feasible proposition. All major network players have agreed to support IPv6 with network modifications. (Microsoft, 2005)

Protocol, Standard and Alliance: Despite its pervasiveness, the current Wi-Fi standards are too power-consuming for many IoT applications, which is why a number of standards groups, such as the Institute of Electrical and Electronics Engineers Standards Association (IEEE) and the Internet of Things Global Standards Initiative from the International Telecommunications Union (ITU), have established many new and low-energy networking standards, protocols and frameworks to help with the development of connected systems. The specific choice of which standard or which combination of standards to use depends on criteria such as data range, security, energy demands and battery life. Bluetooth, ZigBee, Z-Wave, 6LowPAN, and Thread are among the most important standards to date. (DesignSpark, 2015) In 2015, the two previously competing standards ZigBee and Thread established a liaison agreement to work towards a combined solution (ZigBee, 2016). In January 2016, the Wi-Fi Alliance announced that the next-gen Wi-Fi called HaLow would reduce its operating band from 2.4GHz and 5GHz to 900MHz, effectively enabling small payloads and low-power devices (Barrett, 2016). Then in February of 2016, the two previously independent and rival standard groups, AllSeen Alliance led by Qualcomm and the Open Interconnect Consortium (OIC) led by Intel, also joined forces to form the Open Connectivity Foundation (OCF) to collaborate on IoT. Microsoft, Cisco, GE Digital, and Samsung are among the members that are part of OCF. (Open Connectivity Foundation, 2016) The upcoming 5G, the next phase of mobile telecommunication standards, is specifically designed for the scalability, speed, versatility and energy efficiency requirements of the IoT (Kaplan).

SMAC (Social, Mobility, Analytics, and Cloud): In the past couple of years, with the convergence of the social, mobility, analytics and cloud, businesses can now learn the preferences of their customers in real-time and adapt their offerings quickly to create the better customer experience. In particular, SMAC has enabled numerous new IT and business models in recent years and has grown increasingly more sophisticated to prepare for the scale, velocity and variety of the information generated in the IoT era. One significant application for SMAC is in the smart cities. Carlo Ratti, the Director of the SENSEable City Lab, a research initiative established in 2014 at MIT to focus on transforming city services through digitization, described the smart city concept as transforming cities "like 'computers' in open air." He envisioned that the smart cities would empower citizens to plan and manage their lives better by engaging “in a real-time and ongoing loop of information, between the city and its citizens.” (Violino, 2014)
Artificial Intelligence (AI): Long ago, the deluge of data reached the level that it’s impossible for human brains to analyze and utilize efficiently and accurately. The IoT will only exacerbate this problem due to the sheer volume of data created by a rapid expansion of devices and sensors. As of 2008, the number of smart objects already surpassed the number of people on Earth (Marr, 2015). Therefore, the computing platform of IoT should not only communicate seamlessly with humans, and process huge amounts of information in real-time, but also be capable of learning from this data and making intelligent decisions. The prospect in AI has made this a possibly attainable goal rather than science fiction (Balkam, 2015). AI has “enabled computers to understand language, and human-level speech recognition is no longer an elusive goal as it was a decade earlier” as said in the 2014 New York Times bestseller written by two of MIT’s premier thought leaders in their field, Erik Brynjolfsson and Andrew McAfee. Brynjolfsson and McAfee described the current state of technology as in “the second half of the chessboard” where the speed of technology advancement is much faster than in the first half of the chessboard. The exponential growth in technology development will unlock a future where computers and other digital “things” will have “mental power - the ability to use our brains to understand and shape our environments” just like the steam engine and its descendants gave humans substitutes for muscle power. (Brynjolfsson & McAfee, 2014) Gartner, an American research/advisory company, anticipated that by 2017, 10% of computer would be learning rather than processing (Cooney, 2013).
3 Macro Pressures to Innovate

"A problem well stated is a problem half solved.”
- Charles Kettering

3.1 Societal/Consumer Needs

“When your values are clear to you, making decisions becomes easier.”
- Roy Disney

3.1.1 Sustainability Need

“Sustainable development and climate change are two sides of the same coin.”
- Ban Ki-moon Secretary General United Nations

3.1.1.1 Mega Trend 1: Climate Change

In his United Nations Climate Summit speech from September 2014, President Obama said, compared to other immediate challenges such as terrorism, instability, inequality, and disease, the changing climate is an “urgent and growing threat” that “will define the contours of this century more dramatically than any other” (The White House, 2014). According to World Economic Forum (WEF)’s 11th annual Global Risks Report (World Economic Forum, 2016), which analyzed a survey of 750 experts and decision-makers in the WEF multi-stakeholder communities, the risk of failure to mitigate climate change and develop resilience is the most impactful risk for 2016 as well as the ensuing years. In March 2016, Dr. James Hansen, the retired NASA climate scientist, warned that some of the most perilous climate shift consequences such as superstorms and rising sea levels that threaten the world’s coastal cities will happen within decades, not centuries as previously predicted. He also warned that the agreement reached last December in Paris at the United Nations Climate Change Conference is not remotely ambitious enough to prevent this from happening. (Gillis, 2016) Today, the adverse effects of climate change are already felt throughout the world in the heat waves, abnormal weather patterns, droughts and the recent outbreak of Zika virus, causing up to hundreds of billions of dollars of damage (Baehr & Harvey, 2014).

Why is this relevant to the smart home? The answer to this question lies within the understanding of what contributes to the greenhouse gas emissions (GHG) that are causing the climate change. According to a blog post by an independent research group that provides information to help people reduce their carbon footprint, household electricity use makes up roughly about a third of total electricity use and greenhouse gasses emitted in most developed countries (Wilson, 2013). In addition
to electricity, many other major carbon footprint contributors such as food and goods are also often found in the boundary of a home. Moreover, increasingly, the rising popularity of electric cars is moving the energy supply from service stations to garage charging hubs in houses and residential buildings. To date, connected cars have been leading the way to curb carbon footprint in the transportation industry, whereas carbon footprint in households remains a largely unsolved issue for many people (Aman, 2015).

For a while, green products such as Energy Star appliances and efficient light bulbs were seen to be the solution to reduce household carbon footprint. In recent times, however, smart products are bringing energy efficiency to the next level. Sarwant Singh, Senior Partner at the research firm Frost & Sullivan, estimated that smart products can typically provide energy and efficiency savings to users up to 30% more than green products, and users can typically recover their initial investment cost in two to three years. (Singh, 2015) This level of energy reduction is attainable because smart products can potentially integrate sensors and actuators with Internet connectivity into every energy-consuming device. As a result, the energy consumption of a home as a whole, as well as that of individual devices such as HVAC, lighting, fridge, oven, etc., can all be monitored and optimized, giving consumers the tools to better analyze and understand their own energy consumption patterns. Additionally, combining smart home with building retrofitting can help a home significantly reduce its energy requirement and even generate a surplus and contribute energy back to the grid. In fact, energy efficiency is also the number one reason why 58% out of 2,317 US Internet users surveyed in a late 2015 survey conducted by Support.com (a company that specializes in providing technical support for products) would consider purchasing smart home devices (Figure 3-1) (eMarketer, 2016).
For the majority of households, energy efficiency can only be achieved in gradual steps. One such step towards this goal is the widely deployed smart meter, an electronic device that helps utility companies record and manage electricity consumption and distribution in regular intervals (WhatIs - What is smart meter?).

In addition, it's important to realize that even if humanity manages to counter the climate shift for the current and next generation, without new technology to actively reduce GHG already present in the ozone layer, the temperature will still keep rising. Without exit options such as another habitable planet, future generations will most likely have to live more like Singaporeans and spend much of their time indoors as extreme heat surpasses the threshold which the human body can naturally tolerate. Hence, due to climate change, what people do indoors now have a significant impact on the future livability of the outdoors. What this trend seems to suggest is that the indoors will increasingly become more important for a sustainable and resilient future, which makes the smart home a front and center technology application area for the current generation as well as the generations to come.

3.1.1.2 Mega Trend 2: Aging Population

In his talk at Stanford Graduate School of Business (GSB) in 2013, "Five Trends Reshaping the Global Economy," Dominic Barton, the Global Managing Director of McKinsey & Company, highlighted five forces driving the future of the global economy. He said that by 2050, 22% of the global population would be over 60 years-old, twice that of today. (Stanford Graduate School of Business, 2013) That's almost
one out of every four people. Moreover, the aging population issue will be severe all over the world except Africa (Global AgeWatch, 2015).

A 2014 piece in Scientific America says that “smart home sensors could help aging population to stay independent” and IoT applications “could help make seniors more independent by letting doctors or relatives keep tabs from afar.” The technologist Jason Johnson, chair of the Internet of Things Consortium also revealed that many elder care providers are very interested in the technology as they “are seeking to keep the elderly in their homes rather than moving them to assisted-living centers.” Many smart home product examples already exist today such as remotely controlled alarm systems and activity detection devices. These technologies can detect motion or lack of motion, and send alerts to family members, caretakers, and hospital ambulances when an emergency occurs. Additionally, smart appliances can help order groceries online on their own, and smart kitchens can, in the future, make cooking much easier than it is now. (Bruzek, 2014)

Besides making independent life more convenient for seniors, the mobile health trend is moving new care delivery models into the patient’s home as well. Remote healthcare can give doctors real-time biometric data to allow them to treat patients proactively. Telehealth allows lab work such as weight measurement, pulse, and blood pressure readings that would traditionally require on-site visits in a clinic or hospital to be carried out at home. (Counter, 2016) Overall, the smart home can minimize the need for traveling hence transportation cost to users and associated impacts on the environment, consequently lowering the costs of diagnosis and treatment and improving service speed to a great extent.

3.1.1.3 Mega Trend 3: Global Resource Constraints

Another force shaping the future mentioned in Dominic Barton’s talk at Stanford’s GSB is the global resource depletion that has been causing the gradual rising of prices in commodities such as water, energy and food (Stanford Graduate School of Business, 2013). The smart home has a huge role to play in reducing waste through energy/water/food management as evidenced by many innovative smart products in the market today.

Harvard Business School Professor Michael Porter and CEO of PTC Jim Heppelmann (2015), co-published a paper, in which they described the “broader benefits of the IoT” to change the overall consumption patterns. The article says, smart products eventually can be “continually improved, upgraded, and modernized” which allow consumers to keep them longer and will free people to “purchase only the goods and services [they] need, to share products that [they] do not use much, and to get more out of the products that [they] already have.” Another article (2016) in the journal Nature, described a “Circular Economy” as a way of turning goods “that are at the
end of their service life into resources for others, closing loops in industrial ecosystems and minimizing waste.” The article mentioned a joint study by seven European nations, which concluded that “a shift to circular economy would reduce each nation’s greenhouse gas emissions by up to 70% and grow its workforce by about 4%” and the IoT “will boost such a shift, but also demand a policy review that considers questions of ownership and liability of data and goods.” (Stahel, 2016) This concept applies to the smart home because most goods and products people purchase end up in either their homes or their family and friends’ homes.

As evidenced by data provided in this section, the smart home is one of the key enabling technologies to enable a future that is sustainable for all.

3.1.2 Social Need

“You cannot hope to build a better world without improving the individuals. To that end each of us must work for his own improvement, and at the same time share a general responsibility for all humanity.”

- Marie Curie

There are many visions for the future home, but they all seem to be coalescing around the idea that it will be an intelligent, automated home that increases comfort, convenience, and productivity to the extent that it can take care of you instead of you taking care of it. Ideally, the home would be an integral artificial intelligence operating system capable of learning from and adapting to the likes and dislikes of the inhabitants it’s serving as well as to changes in its environment.

While this vision is delightful, it should be added that the potential educational value of the smart home to consumers is even more important given the mega trends discussed in the previous sections. This is because living a sustainable lifestyle is not easy for most people; other unmet needs such as comfort, convenience, and productivity often take precedence in life. In his 2014 book Social Physics: How Good Ideas Spread-The Lessons from a New Science, MIT Media Lab Professor Alex Pentland explained with three examples “health habits, political preferences, and consumer consumption” and concluded that “exposure to the behavior of peers, both direct and indirect, predicted idea flow... Perhaps this is because learning from surrounding example behaviors is much more efficient than learning solely from experiences. Indeed, we will see that providing social network incentives to change idea flow is a far more powerful method of changing behaviors than the traditional method of using individual incentives.” Much of the talk and interest about sustainability occur at the national policy level, but the individual citizens, who could have the most impact on sustainability, are not empowered to make changes in their daily lives. Additionally, social network incentives not only exert influence on changing idea flow but also, as Professor Pentland went on to clarify, “adoption
of habits and preferences is a slow process that requires repeated exposure and perceptual validation within a community of peers." The deeper reason is that for most people, "trust, by which I mean the expectation of future fair, cooperative exchanges, is built from the history of exchanges between people. The pairs of people who had the most invested in the relationship, that is, those who interacted and cooperated the most, were the ones who could exert the most social pressure on each other." The smart home application can be used to increase sustainability awareness through timely feedback and communications on how to save on energy and reduce waste and even the overall cost of living (individual incentives). It can enable the creation of a conducive environment to provide the social incentives needed for a positive feedback loop of social influence for homes and communities to save on resources. A study at Columbia University using adapted social network tests successfully characterized that ecological monitoring and feedback through peer network energy consumption allows users to compare their energy saving habits with those of their neighbors, friends, families, and other community members, thus providing the social incentives needed for positive change (Jain, 2013). Understandably, due to its proximity to end users, home is the best place for smart products to influence behavioral changes.

In addition to the educational value of the smart home, home also bears unique significance on its inhabitants’ emotional and psychological wellbeing, which often permeates into other areas of life such as work.

3.1.3 Economic Need

"Economy has frequently nothing whatever to do with the amount of money being spent, but with the wisdom used in spending it."

- Henry Ford

In 2015, McKinsey Global Institute estimated that "in the United States alone, household activities (cleaning, washing, preparing food, gardening, caring for pets, and so on) and purchasing home goods and services require 230 billion labor hours per year." Worldwide, they projected that "the value of time spent on domestic chores will be more than $23 trillion in 2025." Based on these statistics, an economic evaluation of IoT applications in the home could be as high as $350 billion per year. (Manyika et al., 2015)

Besides the staggering tangible financial implications of existing activities in the home setting, telework is another trend that over time will only increase the economic effects of home. Interestingly, Americans already spend virtually 90% of their lives indoors (Segran, 2015). Historically, this time is divided between work and home; however, more recently, the telecommuting movement is setting this balance in a new direction. In January 2016, the globalworkplaceanalytics.com, a website that
collected a “database of over 4,000 documents on telework/telecommuting, alternative workplace strategies, workplace flexibility, and employee wellness/and well-being ROI,” and who issued regular releases of their research findings on the latest telecommuting statistics, published a new update that stated that “3.7 million employees (2.8% of the workforce) now work from home at least half the time” and “the employee population as a whole grew by 1.9% from 2013 to 2014,” while population of employees who telecommute grew by 5.6%. (Global Workplace Analytics, 2016) In fact, as a remote workforce rapidly becoming the norm, many employers are actively rolling out work from home programs (James, 2015). In other words, relative to time spent at work, the time spent at home is gradually increasing, which increases the value of sustainable innovations in the home setting.

To conclude, as Professor John Sterman said it well in a class, without the environment, there will be no society; without society, there will be no economy (Figure 3-2). And without the economy, what would happen next?

![Figure 3-2: How Environment, Society and Economy Relate to Each Other (MIT Sloan Class "Strategies for Sustainable Business")](image)

### 3.1.4 Objectives of the Smart Home

Among the seven IoT applications listed in Figure 2-1, the smart home is the only innovation, with both existing technologies and new breakthroughs that can help alleviate all the societal/economic needs as discussed in the previous few sections. This establishes the necessity for timely successful innovation into the smart home
space. Combining both these pressures with traditional concepts of home, the goal for the smart home should be:

To enhance personal and facilities’ safety, security and comfort of a home and to prepare for future challenges

By giving users control/feedback/decision support of their energy, food and water usage, in-house healthcare services and other capabilities

Using safe, reliable, secure, sustainable, affordable and easy-to-use connected products.

Security in the above statement refers to cybersecurity because traditional home products are secure from cyberattacks since they are not connected to the Internet. As can be seen, cybersecurity is one of the critical success factors for the smart home innovation, but it’s also a poorly understood one. The reasons behind why cybersecurity in the smart home is poorly understood will be discussed in detail in Chapter 5.

Lastly, energy self-sufficient future homes will inevitably impact some industries more than others; in particular, the utility industry will be affected the most. A 2012 McKinsey study made practical recommendations to utility companies on how to transform their business model to adapt better to the new trend of the future home (Busnelli et al., 2011).

3.2 Business Pressures

“Companies are like sharks. If they stop moving, they die.”

- Salesforce.com Chairman Marc Benioff

3.2.1 Technology Incumbents Quandary

In late 2015, Accenture conducted a survey on the use of consumer technology (a traditionally highly profitable global industry involving more than $200 billion) with 28,000 consumers representing the online population across 28 countries in six continents. The study found that globally, the smartphone market has reached maturity just like the markets for tablets and laptop computers. (Accenture, 2016) Electronic technology follows the technology life cycle (TLC) and typically has a short lifespan; after it reaches the maturity stage, what comes next is that business gain will decline (Wikipedia - Technology Life Cycle). Naturally as a result, large public tech and telecom companies saw the IoT as the next wave to drive revenue over the next few years and possibly decades.
Furthermore, it's important to remember that each incumbent consumer tech company has a large ecosystem of partners, suppliers, customers and employees behind it that will be affected by the winding down of the traditional digital products if the company cannot generate further revenue growth. If that's the case, because these incumbents have amassed substantial relative advantage over competing businesses, they may easily forage into other industries, potentially creating a large rippling effect across the economy.

Because the demand is slowing down for the established digital categories, high-tech consumer incumbents have more motivation to innovate and expand into the IoT, the next generation of devices to sustain growth. Also with the IoT, these companies can leverage their customers in the existing value chain. As we've seen in recent years, large tech companies have been conducting some wide-reaching acquisitions as well as investing in internal innovation efforts. Specifically, in the smart home space, Google acquired Nest, a smart thermostat maker, in January 2014 for $3.2 billion. Months later in August, Samsung acquired Washington DC-based SmartThings for $200 million. (Tilley, 2014) In 2015, Alphabet/Google announced the Brillo OS and Weave platforms, a response to Apple's HomeKit (NextMarket Insights, 2015). Then there was the release of Google's OnHub Wi-Fi router (Kastrenakes, 2015), and Amazon's launch of Echo/Alexa, which became a bestseller in the home automation world (Risley, 2015). Apple, on the other hand, took a homegrown approach and built its own SDK HomeKit to enable developers to create new applications in its ecosystem, and more recently, Apple open-sourced its Swift language (new programming language for iOS, OSX, watchOS, and tvOS) (Evans, 2015) and Amazon's investment of $100 million in developers to build new apps for its Echo platform (Risley, 2015). In essence, technology incumbents all made significant financial strides on smart home innovation to compete on building the next smart home ecosystem.

### 3.2.2 Global Competition

In 2015, a report published by the McKinsey Global Institute found that global competition is escalating due to the rising of emerging-market companies, and many technology and technology-enabled firms have become agiler to make rapid moves into new sectors. In the past three decades, the world's largest corporations have been riding an unprecedented "wave of profit growth, market expansion, and declining costs." As a result, the corporate-profit pool had increased from 8% of global GDP to nearly 10%. However, this wave is going towards a descending trend for the next ten years, and the corporate-profit pool could shrink back to less than 8% by 2025, virtually undoing all the gains from the previous three decades. As the report noted, the "competitive landscape has grown more complex, and the pace of change is accelerating," as new competitors grow to be "more numerous, more formidable, and more global - and some destroy more value for incumbents than
they create for themselves.” The report postulates that “as profit growth slows, there will be more companies fighting for a smaller slice of the pie.” (Dobbs et al., 2015)

3.2.3 Rising Consumer Demand

Additionally, while technology has improved the quality of life and benefitted many businesses, it has also resulted in customers demanding a “fast, cost-effective and personalized level of experience,” with which 97% of US business leaders agreed in a survey by Lithium in May 2015 (Figure 3-3). The same survey also indicated that “nearly two-thirds of corporate execs said rising customer expectations had increased pressure to innovate.” As a result, companies were spending more to keep up with consumer expectations. The current push into the IoT is one example of such consequence. (eMarketer, 2015)

<table>
<thead>
<tr>
<th>Ways in Which Rising Customer Expectations Have Affected Their Company According to US Corporate Executives, May 2015</th>
<th>% of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased pressure to innovate</td>
<td>65%</td>
</tr>
<tr>
<td>Increased competition with other companies</td>
<td>58%</td>
</tr>
<tr>
<td>Increased costs to serve the customer</td>
<td>52%</td>
</tr>
<tr>
<td>Increased customer turnover</td>
<td>30%</td>
</tr>
<tr>
<td>Slowed revenue growth</td>
<td>29%</td>
</tr>
<tr>
<td>Increased the amount of discounts my company provides to customers</td>
<td>28%</td>
</tr>
<tr>
<td>Reduced our market share</td>
<td>17%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
<tr>
<td>None</td>
<td>4%</td>
</tr>
<tr>
<td>Not sure</td>
<td>3%</td>
</tr>
</tbody>
</table>

Note: n=311
Source: Lithium, “Executive Omnibus” conducted by Harris Poll, June 2, 2015

Figure 3-3: Effects of Customer Expectations on Companies (eMarketer, 2015)
3.3 Causal Loop Diagram

In summary, all the factors explained in this chapter point to the high pressure and the urgency to innovate into the smart home space. Figure 3-4 is an adaptation from Figure 1-2 and Figure 1-3 with added linkages among the pressures explored in this chapter.

Several major changes in this adapted model are:

1. To make the kinds of results that are expected in the smart home innovation clear, the “results” variable is expanded into three new variables “Attractiveness of the Smart Home,” “Smart Home Install Base,” and “Value Captured in the Smart Home.” These variables are highlighted in blue. The assumption is that the more effort allocated to the smart home innovation, the more attractive the smart home products will be to consumers, and as a result, there will be more
install bases (sales). The increase in the smart home devices sold then in turn increases the value captured in the smart home.

2. The "Managers' Goal for Commitment" variable is expanded into the two new loops B3 and B4. Both new loops and all the new variables are highlighted in orange. The new loop B3, "Major Challenges Facing Our Time," summarizes the dynamic factors described in Chapter 3.1. The challenges include sustainability challenges in both environment and business. The societal/consumer needs factors increase the need for timely successful smart home innovation, which pushes the industry to close the smart home commitment gap, which after traversing the links in the normative pressure loop and the innovation reinforcement loop, lead to a reduction in societal/consumer needs. Similarly, the loop B4, "Next Wave," captures the dynamics where the business pressure to innovate increases the time-to-market requirement for the smart home innovation, which, after traversing the links in the normative pressure loop and the innovation reinforcement loop, leads to a reduction in business pressure to innovate.
4 Growing Peril of Cybercrimes

"Technological progress is like an axe in the hands of a pathological criminal."

- Albert Einstein

Cybercrime or computer crime is defined as “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks” (Halder & Jaishankar, 2011). According to PwC, a multinational professional service company, the number of detected security breaches has been growing at a steady double-digit rate year after year for the past five years. In 2015 alone, the number has jumped 38% over 2014. (Wong, 2016) Because the number of IoT devices is expected to grow dramatically in the next few years, it’s obvious that the number of incidents will dramatically increase as well since there will be many more devices to hack. Appendix A – E show the latest research findings from Symantec’s 2016 Internet Security Threat Report and Dell SecureWorks’ 2016 Underground Hacker Market report.

Before the annual WEF meeting in Switzerland in 2015, WEF along with Deloitte published a framework, called “cyber value-at-risk,” to help organizations unify different cyber risk factors and quantify the value at risk in case of a cyberattack. The framework introduced three principal constituents to assess cyber risk factors: 1) the profile of the attacker based on who the attacker is and their motivations, 2) the vulnerabilities and defenses in the enterprise, and 3) the assets under threat. (Prince, 2015) The following three chapters (4, 5 and 6) adapt this framework and apply it to the emerging smart home market. This chapter focuses on the first constituent: the profiles of cyber attackers.

4.1 Types of Cyberattacks

"Cyber attacks are not what makes the cool war ‘cool.’ As a Strategic matter, they do not differ fundamentally from older tools of espionage and sabotage.”

- Noah Feldman

4.1.1.1 Reconnaissance

There are many categorizations of the types of attacks. One such categorization is by targeted and non-targeted attacks. The difference between targeted and non-targeted attacks is that targeted attacks often have a planning phase called reconnaissance. Intruders engage with the targeted system to get information about
vulnerabilities such as a list of possible attack vectors (a path or means by which a hacker can gain access to a computer or network to cause a damaging outcome) that can be exploited later for further attacks. Reconnaissance uses computers as a tool to obtain information including technical vulnerabilities such as the targeted private network's hostnames, IP addresses, and various internal path names and non-technical vulnerabilities such as the names of the people involved. One typical method conducted in the reconnaissance step is port scanning or penetration test to locate system vulnerabilities. (WhatIs - What is active reconnaissance?)

4.1.1.2 Social Engineering

Social-Engineer.org defines social engineering as “any act that influences a person to take an action that may or may not be in their best interest” (The Official Social Engineering Portal). Frequently, a social engineering attack follows a reconnaissance where an attacker tries to trick or manipulate the most beneficial social vulnerability that results in the disclosure of confidential information, the breaking of normal security procedures or other desired outcome to the attackers. In other situations, social engineering is the first step in an attack plan. With social engineering, the cybercriminal will first try to gain a victim's confidence and trust; once they succeed, they can get the information they need for the next stage of the attack. Spam and phishing are probably the most common type of social engineering. They are unwanted email messages whose goals typically range from minor annoyance to malicious links that lead to malware-infected websites to bait that is too good to be true. Bait is a financial promise such as an announcement of winning a lottery that the receiver never subscribed to or a fake business proposal. (Khanse, 2014) Both spam and phishing use computers as a tool to infect the target, and can be carried out much more efficiently than they ever were through computer programs. For cybercriminals, tricking humans is often the easiest way to gain access. In fact, in the majority of the breach cases, an employee accidentally clicks on a phishing link containing malware that is automatically downloaded, and the malware enables cybercriminals to steal the employee's access credentials to an internal network, in turn giving these criminals access to proprietary data.

4.1.1.3 Identity Fraud

This type of cybercrime often happens after the reconnaissance step or after the social engineering step when an attacker obtains the information needed for the next step of his/her targeted attack or it could be the first step in non-targeted attacks. Often, identity fraud is the end goal for the attack. Identity fraud and spam along with phishing described in the last section are among the most common types of cybercrimes (Khanse, 2014). Identity fraud is caused by data breaches where a criminal uses sensitive personal information for financial gains.

4.1.1.4 Malware

43
Malware stands for malicious software because the software's creation intent is malicious. Software that causes unintentional harm due to defects is not malware. Malware is used to disrupt computer use, gather private data, and gain access to internal computer systems. There are many different types of malware. In some cases, malware is sneaky, as it can be embedded in legitimate-looking programs, intending to steal information rather than causing immediate harm; these are Trojans and are hard to detect. (Wikipedia - Malware) In other cases, Trojans or other malware can be used to carry out a denial-of-service (DoS) attack. DoS intends to bring an online service down by overwhelming the system limit with massive traffic, which can come from many locations and sources. These attacks target computers rather than individuals. Any connected device can be leveraged to carry out DoS attacks. In particular, a botnet is an array of compromised private computers infected with malware controlled as a group to send spam messages or carry out other malicious tasks such as the distributed denial-of-service (DDoS) without the owner ever knowing. DDoS is a type of DoS where multiple systems infected with a Trojan are used to conduct DoS attacks on a single system. (Khanse, 2014) The longest standing form of malware is probably computer viruses, software that can self-replicate and move into other computer programs, data files, and even the hard drive to cause widespread harm. A computer worm takes the virus to the next level because it can spread itself to other computers through the network. (Wikipedia - Computer Virus) Such is the latest case of Stuxnet, a computer worm that specifically targets critical infrastructure; it wiped out one-fifth of Iranian nuclear centrifuges in 2009 (Nakashima & Warrick, 2012). The newest arrival of malware is ransomware, a type of malware that extorts a payment from its victims by locking their systems and data. Specifically, crypto-ransomware, one type of ransomware, is particularly damaging; crypto-ransomware encrypts all personal files on an infected computer and holds the private keys to the decryption until the owner of the computer makes a payment. Crypto-ransomware Cryptolocker discovered in 2013 had scooped $27 million in ransom paid during a short period of two months (Zorabedian, 2015). Ransomware like other types of malware uses social engineering to infect computers. Recently, the threat of ransomware is quickly growing. Cyber Threat Alliance, a group of cybersecurity experts, estimated that the recent CryptoWall has victimized hundreds of thousands of users worldwide and stolen more than $325 million so far (Drolet, 2016). Dell SecureWorks has uncovered nearly 625,000 CryptoWall infections, 250,000 incurred in the US alone, in less than half-a-year period in 2015 (Simonite, 2015). Also in 2015, the FBI reported a total of 2,453 ransomware complaints and a loss of $24.1 million, nearly one-third of all of the complaints reported in the last ten years (Abdollah, 2016). Even though malware attacks can be both targeted or non-targeted, according to Symantec’s 2015 Internet Security Threat Report, non-targeted attacks still make up the majority of malware, an increase of 26% from 2014 (Symantec, 2015). The reason for this imbalance of attack types is probably because non-targeted attacks are easy to carry out due to poor security in many devices. A watering hole attack uses a combination of social
engineering with malware that targets a particular group rather than individuals. In watering hole attack, an attacker finds out which websites a group often visits either through social engineering or reconnaissance and infects it with malware with the ultimate goal that this malware will infect part or all the group members after they revisit the site (Donovan, 2014). The term drive-by download attack is used to describe how malware can infect users' computers simply because the users visit a website that is running malicious code (Khanse, 2014). Barely into 2016, the Ukraine power grid attack and the Hollywood Presbyterian Medical Center attack showed that cybercriminals are willing to put lives at risk for national causes and financial gains (Gupta, 2016).

4.2 Attacker Profiles

“The only thing more expensive than education is ignorance.”

– Benjamin Franklin

Just as the types of attacks vary quite a bit, the classes of cyber attackers also span a wide range and can be best categorized by their motivations (Figure 4-1) as described in an article posted on the Technology Innovation Management Review. According to the authors, cyber attackers can be broadly divided into

1) “Insiders” include:

   - **Disgruntled employees** may retaliate due to holding grudges;
   - **Thieves** may misuse their privilege as insiders for personal financial gains through the manipulations or misuse of company’s electronic assets;
   - **Unintentional insiders** may unsuspectingly facilitate outside attacks.

2) “Outsiders” include:

   - **Organized attackers** include terrorists, hacktivists, national states, and criminals;
   - **Hackers** may or may not possess malevolent intentions, and comprise black hats and white hats.
   - **Amateurs** are frequently referred to as “script kiddies” or “noobs” and are motivated primarily by curiosity to explore and learn or solve challenges. (Han & Dongre, 2014)
Among the cyber attackers with malicious intent, the main motivations fall into one of the following three categories: 1) financial gain, 2) furthering a geopolitical cause, and 3) media attention. Among these groups of attackers, organized attackers such as the national states and criminal organizations are the best funded and most innovative. (Han & Dongre, 2014) But overall, the sophistication of the hacking trade is improving at a rapid pace across the board (Weisbaum, 2016).

4.3 Current Trends

"Because there are little to no consequences for conducting cyberattacks, criminals and nation-states are becoming bolder in their threats and behavior."

- Michael McCaul

In the PwC's report, "Global State of Information Security Survey 2015," it finds that global security incidents had outpaced both global smartphone users' growth and global GDP growth by a factor of two (PwC, 2015). Many recent trends have fueled this rapid growth of digital breaches.

4.3.1 Thriving Underground Ecosystem

In particular, by using the anonymous Tor network and limiting access to an invitation-only basis, criminals have created thriving cyber underground marketplaces that are almost completely hidden from the public scrutiny. In a 2015
article, security researchers Lillian Ablon and Martin Libicki at the RAND Corporation noted that the hacking trade has become much more specialized in recent years. There is an entire underground ecosystem of sellers and buyers who can “deal freely in its tools and spoils” such as exploit kits, botnets, compromised hosts, and a massive amount of stolen credit-card numbers and other personal credentials and "as-a-service" offerings (hacking for hire). (Ablon & Libicki, 2015)

**Exploit Kits:** In particular, cyber breaches have become both much more sophisticated and easy to carry out for malevolent actors, due to fast growth and wide availability of inexpensive exploit kits for creating, disseminating and managing attacks, as well as powerful distributed system technology. Kevin Haley, a Director at Symantec Security Response said in an interview with NBC News that "In 2009, we had about two million pieces of malware and at the time we thought that was pretty overwhelming, and now we're talking about more than 430 million. It's more than a million new pieces of malware getting written each and every day" (Weisbaum, 2016). Among the released malware every year, ransomware alone doubled between 2013 and 2014, and the amount of crypto-ransomware had grown to be over 45 times larger. In fact, to access cyber weapons, all one would need is an Internet connection and a few hundred to a few thousand dollars' cash. For example, a toolkit to carry out drive-by download attacks as mentioned earlier can be rented for between $100 and $700 per week with 24/7 customer support and free software updates. The online banking malware SpyEye (also known as Trojan SpyEye) can be leased from $150 to $1,250 for a six-month term, and DDoS exploit kits cost from $10 to $1,000 per day. A Trojan with remote access only costs between $5 and $10. (Symantec, 2015) Furthermore, the prices of the cyber weapons have been plummeting; the cost of launching a DDoS attack is down to about $38 per hour. At the same time, the damage of unmitigated attack for businesses is growing to $40,000 per hour according to cybersecurity firm Incapsula. (Griffiths, 2015)

**Services:** Moreover, hackers sell "cybercrime as a service" such as "I can infect X computers for a fixed price of Y." For example, it costs only $500 to break into a corporate mailbox, and even less about $350 to break into a website, $129 to break into a Gmail/Yahoo account, and $90 to get a victim's IP address. DoS attack services have a metering business model: $5 to $10 for an hour, $30 to $55 for a day or $200 to $555 for a week. Stolen data prices, with the exception of online bank account details, which have remained stable, have declined. For example, email prices have declined considerably, and credit card information has also dropped. (Symantec, 2015) In 2014, a so-called Fullz (full information package) including name, address, credit card information, date of birth and more costs about $35 to $45, and this price was down to merely $20 in 2015 (Solomon, 2016).
Lessons: Just as there are online classes and YouTube tutorials on the application of every legal technology tools in the wild, the underground market also sells hacking tutorials for between $20 and $40 (Solomon, 2016).

The point is that the markets for cybercrime tools and stolen data have become so pervasive and accessible that the nefarious hacking trade today has become more lucrative and easier to carry out than most people would imagine (Ablon & Libicki, 2015).

4.3.2 Compromise Efficiency vs. Discover Efficiency

Another issue is the growing innovation gap between attacker efficiency and defender efficiency over the past decade. Verizon's 2015 Data Breach Investigation reports that attacker efficiency was 75% in 2004 but increased to around 90% in 2014, whereas the efficiency to detect attacks within days only improved from approximately 11% to 20% over that same period. In Figure 4-2, the orange line shows how often attackers are able to compromise an organization in days or less, and the teal line shows how often defenders are able to discover compromises within that time. The report also noted that in 60% of cases, compromises happened within minutes. (Verizon, 2015)

![Figure 4-2: Compromise vs. Discover Efficiency](Verizon, 2015)
In part, this is because once a malware is created, it can be used to infect tens of thousands to millions of devices as illustrated in the case of Darloz, a new Linux malware that specifically targeted small Internet-enabled devices such as "home routers, set-top boxes, and security cameras." Darloz was discovered near the end of 2013 by Symantec researchers, and barely three months later, by March 2014, Symantec identified 31,716 devices infected with the malware. (Symantec, 2015)

4.3.3 Known Vulnerabilities

In the past decade, open source software has become very popular in the corporate world of IT and R&D. Many internal and external applications rely on the assembly of these off-the-shelf software packages, since integrating this software will often make more economical sense than developing something in-house from scratch. In fact, the open source movement has leveled the playing field for many companies, but the problem is that many open source packages have publicly known vulnerabilities, and as many devices incorporate the same open source components, the vulnerabilities in a component can affect every software application that integrates it. These vulnerabilities are one of the biggest threats for IT departments and sometimes their customers. HP's 2015 Cyber Risk Report found that 44% of 2014 breaches came from vulnerabilities that are two to four years old (Drolet, 2015). In 2014, researchers found a security defect called Heartbleed, in a common security software component used in many critical systems from weapons systems to home Wi-Fi routers by companies such as Amazon, Netflix and Yahoo, and even the FBI and the Pentagon. Later that same year, researchers discovered another serious flaw, named Shellshock, in a program that is commonly used by 70% of Internet connected machines. Due to the widespread use of these two pieces of software, these two security issues affect more than half of the Internet. (Perlroth, 2014)

Besides open source packages, software by commercial vendors also poses a serious threat. An Italian company Hacking Team, which sells surveillance and intrusion software to governments, companies, law enforcement and security agencies, was itself hacked in July 2015, resulting in a release of 400GB of company data. Found among the leaked data were some "zero-day" exploits (security flaws in popular software previously unknown to their vendors, and therefore, unpatched) such as a Flash vulnerability. Within hours of the public release of the zero-day flaws, exploits that targeted these flaws were folded into an array of existing malware and hacking frameworks in the wild. (Goodin, 2015) As can be seen, software not only needs the proper configuration that avoids giving attackers an easy way in but also must be patched by both its vendor and its users promptly after a public exposure of vulnerability.
4.3.4 State-sponsored Groups

As a result of the trends described in the previous sections, many countries have begun collecting computer weapons on an unprecedented scale, and state-sponsored groups are on the rise. According to Wall Street Journal research conducted with some US and foreign officials, at least 29 countries have dedicated military, or intelligence units to belligerent cyber hacking efforts, which means many organized hacking teams are well-funded by their governments. In comparison, many security defense operations in corporations find it difficult to match the sophistication of organized crime. In fact, some 50 countries have bought readily available hacking software, like that sold by the Italian firm Hacking Team, mentioned in the previous section. Countries use Hacking Team’s software for domestic surveillance and international espionage. Pakistan and India, two nuclear-armed neighboring rivals, regularly attack each other’s companies and governments. Estonia and Belarus are building a cyber defense to counter Russia’s cyber bullies. Denmark, the Netherlands, Argentina, and France are developing programs to develop offensive cyber weapons. Governments can use cyber weapons to mine and steal information from each other, erase data on computers, knock out electrical grids, disable domestic airline networks, perpetrate DoS attacks, disable bank networks, erase money from bank accounts, and even destroy nuclear centrifuges. (Paletta et al., 2015) Many of the most advanced recent cyberattacks, such as the Stuxnet attack, appear to be carried out by national states (Nakashima & Warrick, 2012). As of today, besides the US, Russia and China have the most sophisticated cyber programs, according to the Director of the United States’ National Intelligence James Clapper (Ackerman & Thielman, 2016).

4.3.5 Digitally “Savvy” Next Generation

Near the end of 2015, an article in The Guardian reported that the desire for status is luring many teenagers to perpetrate cyberattacks, and the average age of attack suspect has dropped from 24 to only 17 in a period of 12 months. In one case, a 12-year-old bought a Blackshades virus, a Trojan-like program that allows the attacker to take control of another computer secretly. (Association, 2015) In 2014, a 14-year-old demonstrated that he was able to hack in and control a car with a device he assembled overnight using $15 worth of Radio Shack parts (Mearian, 2015). The point is that hacking is not as difficult as many people might think. And suffice it to say, if there are not enough incentives to keep the digitally savvy future generations on the right side of the law, there will be plenty more cyberattacks coming in the future.

4.3.6 Cybersecurity vs. National Security

As of today, in the US and the UK at least, national security comes before cybersecurity. In 2015, a group of computer scientists and security experts warned
the US government in a technical report by MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL), that backdoor surveillance would “pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations.” The report argues that if the US government has access to personal data, so can other governments, cybercriminals, and terrorists. The report uses the case in 2010 when Google’s database, built for the purpose of meeting the government’s requirement for backdoor surveillance, was hacked by the Chinese government for their surveillance as well. (Abelson et al., 2015) Recently, many companies have upped their game in their encryption efforts. One such example is Apple, as seen in the recent heated public debate between encryption and surveillance in the Apple vs. FBI case. The FBI has been demanding that the US government impose a stronger restriction on encryption. (Brandom, 2016) However, unbeknownst to many, lack of encryption is one of the main causes for many technological security failures of today. One recent report from the Harvard Berkman Center for Internet and Society explored both sides of this debate (The Berkman Center for Internet & Society at Harvard University, 2016). Another research report from the Berkman Center pointed out that restriction on encryption would not work, as “bad guys can easily switch to foreign encryption products that don’t have backdoors” (Brandom, 2016). This debate is still ongoing, and it is not clear which side will win the argument in the end. But what is clear is that government policy on encryption will play a significant role in the future direction of technological innovation on the Internet.

4.3.7 Quantum Computing

In reality, with the speed of quantum computing development, some widely used encryption methods may soon be obsolete. Already in 1994, mathematician Peter Shor showed that a prototypical quantum computer would be able to crack relatively easily the RSA encryption, a public-key encryption technology developed by RSA Data Security Inc. RSA is the de facto standard for encryption used to safeguard today’s Internet traffic. With RSA, a sender uses a public key to encrypt a message, and only a secret key possessed by the recipient can decrypt the message. The security of RSA is only as strong as the security of the private key, which is typically a very large number. With conventional computers, the larger the number, the more difficult it is to break it into its prime factors. But quantum computers will change that as they could factor a large number exponentially faster than any existing computers. In 2016, a group of scientist from MIT and the University of Innsbruck in Austria have demonstrated they can implement the Shor’s algorithm the first time with scalability. (Chu, 2016)
4.4 Causal Loop Diagram

Figure 4-3 incorporates the increasing sophistication of the cyber attackers to the causal loop diagram from Figure 3-4. Four new variables that coarsely summarize the details in this chapter are “Sophistication of Attackers,” “Easiness of Carrying Out Attacks,” “Number of Cyberattacks,” and “Number of Cyberbreaches” (highlighted in orange). The assumption here is that the number of cyber breaches will decrease the attractiveness of the smart home. This assumption will be supported with additional data in Chapter 6 where feedback will be added to close the loops involving these new variables.

Figure 4-3: The Impact of the Escalation in Cybercrimes on the Smart Home
5 Vulnerabilities in the Smart Home

"So in war, the way is to avoid what is strong and strike at what is weak."

- Sun Tzu

5.1 Current Attack Scenarios

"Home is where the heart is."

- Pliny the Elder

At the 2015 International Consumer Electronic Show (CES), Edith Ramirez, the Chairwoman of the Federal Trade Commission (FTC), said that any connected device is subject to hijacking. Furthermore, she added, the risks of breaches intensify as more and more sensors connect devices (such as cars, medical care, and homes) that are impactful to our physical safety to the Internet. (Wood, 2015) In a somewhat similar message, the FBI’s chief information security officer Arlette Hart warned that the impact of IoT cyber breaches could have much worse consequences for consumers than previous enterprise breaches. She said the attack surface is much larger than ever before as there are more devices to secure and the downsides from failure are dramatically increasing as well. (Eckerson, 2015)

In particular relation to cybersecurity for the smart homes, Prof. Udo Helmbrecht, the Executive Director of the European Union Agency for Network and Information (ENISA), suggested that the smart home market was evolving at a rapid pace. He said that embedding connectivity to an existing home environment would open new security challenges with safety implications for the smart home inhabitants and visitors. He suggested that ensured safety only come if manufacturers and developers secure the entire lifecycle of their products. (ENISA, 2015)

Since as early as 2013, numerous security and technology research firms have studied a wide range of proof-of-concepts or real attack scenarios on traditional devices as well as new innovative products in the smart home space. In a report released in March 2015, Symantec examined 50 consumer smart products including smart thermostats, smart locks, smart light bulbs, smart smoke detectors, smart energy management devices, and smart hubs. Symantec found that none of the devices verified authorization before connecting, and one out of five devices transmitted unencrypted communications and many allowed unrestricted password tempering. (Lemos, 2015)

The first proven cyberattack on the smart home dated to as early as 2014 when leading security-as-a-service provider Proofpoint published a report about a
coordinated attack campaign that turned more than 100,000 compromised everyday consumer devices such as home routers, connected multimedia centers, TVs and at least one refrigerator into a “thingbot.” A “thingbot” is an Internet-connect embedded system that is infected with malware and coopted into part of a botnet. The “thingbot” sent more than 750,000 malicious phishing and spam emails in a period of two weeks to individuals and enterprises worldwide. Many of these smart home devices were left completely exposed on the public network for criminals to use because they were misconfigured and used the default password. Proofpoint warned that such “thingbot” networks were likely to become more prevalent since IoT devices are typically not protected and are much easier to penetrate than PCs. (Proofpoint, 2015) In fact, later that year in December 2014, one of the largest DDoS attacks to date took down the online gaming services of both Microsoft and Sony for days, proving Proofpoint’s foresight. A Chinese security company NSFocus researched this case and concluded that 30% of the attacks originated from networked devices such as home and office routers that were open to infection by attackers because the default passwords on these devices remained unchanged. NSFocus found 7 million connected devices that could be controlled in the same manner to launch similar scale attacks during a two-day period. (Simonite, 2015) Only a few months later, a US-based web security firm Incapsula found a botnet of more than 40,000 routers through an investigation about a series of DDoS attacks targeting its customers. The routers involved were deployed to their customers insecurely using default credentials by ISPs around the world allowing them to be infected with multiple DDoS malware and controlled by multiple hacking groups. (Constantin, 2015) Another study by Nominum, an American security software firm, found that 24 million home routers on the Internet exposed ISPs to DDoS attacks. Compromised devices are of particular interest to attackers because they allow them to mask their identities and the real source of attacks. (IFSECGlobal, 2014)

The fastest growing smart home segment in the past few years is probably the smart TVs. According to Consumer Technology Association (CTA), as of early 2016, about 46% of the US households had a smart TV and this figure is expected to surpass 50% by the end of the year. CTA also forecasted that nearly 70% of all TVs sold in the US this year will have Internet connectivity. (Weisbaum, 2016) Smart TVs are vulnerable to cyber breaches due to an array of outdated software libraries with known security issues, a lack of anti-virus protection, and the intrinsic assumption that nobody on the same network would ever have malicious intent. Attackers can exploit these flaws to gain access to everything connected to the home network as demonstrated by security firm Avast last year (Young, 2016). Later 2015, in a Symantec blog post, Candid Wueest, a security threat researcher, described the different methods to hack modern smart TVs. He also explained the reason why cybercriminals would want to hack the smart TVs, and those reasons basically fall into one of three categories: getting financial rewards, accessing other connected devices, and recruiting for a botnet. He demonstrated that he was able to infect his new smart
TV with ransomware as he recounted what happened after the infection. The malware "locked the TV after a few seconds, displayed the dreaded ransom note on the screen, and made the TV unusable." (Wueest, 2015)

As previously discussed, home routers and printers were targeted for DDoS because they've been widely deployed and poorly secured, so it's easy to find a relatively large number to launch DDoS which requires a lot of computing power. Another type of attack does not require as many compromised devices but is no less damaging. Created in 2009, Shodan, the world's first IoT search engine, allows users to easily search for pictures with complete IP addresses and timestamps from unsecured webcams around the world (Mohdin, 2016). In 2012, security flaws common in 20 models of TRENDnet's IP-connected cameras were exploited, and consequently, hackers posted links to the live feeds of nearly 700 of the cameras. The feeds showed "babies asleep in their cribs, young children playing, and adults going about their daily lives." (Bartz, 2013) Two years later in May 2014, the situation had not changed much. A "creepware" (hacked webcams used to spy on people) case resulted in the arrest of more than 90 people across 19 countries. (Perez, 2014)

In addition to infested home routers, widely exposed smart TVs, and remotely controlled home cameras, in 2014, IOActive, Inc., a leading security service provider, announced that it had found several security weaknesses in Belkin WeMo Home Automation devices that could impact more than half a million users. The WeMo product let users add connectivity to any other devices in the home such as sprinkler system, thermostats, and antennas. The vulnerabilities allowed perpetrators to perform an unauthorized firmware update that gave them the ability to 1) monitor home occupancy, 2) control smart home devices on the home network just like users can, and 3) attack other devices on the same home network. In the worst scenario, these attacks can lead to possible blackouts and home fires, and even loss of life. (Kerr, 2014)

Another smart home device with the potential to cause catastrophic consequences such as the harming of human life is the smart meters. As of 2014, Edison Foundation's Institute for Electric Innovation (IEI) estimated that utilities have installed 50 million (about 43% of all homes) in US homes nationwide (IEI, 2014). In their book, Sorebo et al. (2011) expressed great concerns about the vulnerabilities in the smart meters by saying that when a virus or worm infects a smart meter, it could allow hackers to gain control of all customers' devices at once once they have access to the network and even cause widespread blackouts. The authors warned that widespread power outages themselves could take weeks or perhaps longer to restore, and that switching the power off and on repeatedly could potentially cause damage to generators, transformers, and other equipment involved including the smart meters themselves and major appliances in homes and other buildings on the same network. In those cases, the consequences could be much more severe than
simple access to data manipulation such as turning off electricity, stealing energy, or even a power outage because the resulting damage to expensive equipment would lead to replacement times that could last longer than a year. (Weaver, 2015)

Perhaps, one would typically expect the attack scenarios where compromised connected products expose other devices on the same network to attack as described in the previous paragraphs apply to what people would often refer to as the gateway systems such as the WeMo device or the smart meters. But in reality, any product, once connected to a smart home network, can serve as the jump-off point for hackers to get control of an entire network. Once a hacker gains access to a network, potential damage is not just limited to personal privacy but also to the safety of the inhabitants and their personal belongings. For example, seemingly innocuous devices such as connected lightbulbs have unique roles in issuing and relaying commands to other devices within the same network. A hacker could trick a connected lightbulb into giving out the network keys which then give the hacker control of the entire network. (Armentrout, 2015)

More recently in 2016, a group of connected products that are purported to improve home security is, in reality, making the home more susceptible to penetrations. The underlining issue with many home security systems is that they use a common sensor which contains vulnerabilities that are unfixable with software updates. SimpliSafe, for instance, is a “smart” alarm provider with more than 300,000 existing customers. In February this year, it was demonstrated by IOActive, the security provider mentioned earlier, that anybody with off-the-shelf hardware and software bought for between $50 and $250 could control the alarm from up to 200 yards away and open the home for burglars and thieves. Furthermore, Samsung’s SmartThings home security devices and Comcast’s Xfinity service have also been reported to have unfixed vulnerabilities. (Fox-Brewster, 2016) In another case, researchers have discovered in early 2016 that IoT doorbells gave home owner’s Wi-Fi passwords to anyone with a screwdriver (Vaas, 2016).

Furthermore, remember the story in the introduction of this thesis about the Scorpion episode? The scenario is not entirely a fictitious TV drama given the current state of the art of the building automation systems (BAS). The scenario was already documented in a published research report back in 2014 when some researchers who attended the Hack in the Box (HITB) conference in Amsterdam warned about “novel scenarios” like remote accessing smart sensors for mass surveillance, or remote locking buildings and holding the people inside for ransom. A research paper titled “Envisioning Smart Building Botnets” described how BAS botnets could allow attackers to cause significant damages to an entire region, even economies by turning them into part of itself. The research paper noted that in the US, there were more BAS than any other automation equipment, and even listed seven BAS botnet attack scenarios. (Storm, 2014)
Finally, the vulnerabilities of smart home devices are also reflected in some recent research statistics. In 2015, PwC found that breaches on Internet-connected devices jumped 152% from the previous year (Wong, 2016). That same year, researchers at security firm Synack analyzed the security states of 16 smart home devices from cameras to thermostats and proved that they could hack almost every device, with smart cameras being the least secure. What’s more is that a successful breach only took several minutes. (Kieler, 2015) As all the above examples illustrate, the smart home devices often have weak or no security measures whatsoever and therefore as their popularity grows, they are making homes increasingly more vulnerable for cybercrimes.

5.2 Sources of Vulnerabilities

“Complexity is the worst enemy of security.”

- Bruce Schneier, CTO of Resilient Systems

5.2.1 Product Vulnerabilities

5.2.1.1 Characteristics of Everyday Objects and Their Security Implications

A seamless digitization of the household would require the smart home products to match up to the characteristics of their conventional counterparts so they can drive demand in a market of millions if not billions of consumers. The everyday objects in a household have four fundamental characteristics that need to be maintained by their smart substitutes. The following paragraphs describe these characteristics and their security implications.

**Functional Role:** Each everyday object already has pre-determined functional roles. Lights are used to light rooms as fridges are for food preservation. None of the smart home products are trying to change their conventional counterparts’ existing roles dramatically. Instead, smart products add connectivity and data gathering and processing capabilities in addition to existing functions to create more value for their users. Simply adding connectivity is an incremental innovation as it does not change product internals and the way the internals used to work together before. As a result, the sensors that make things “smart” need to fit in with existing components of every product they try to transform. This requirement puts a design constraint on the feasible sizes of sensors. Another problem is that once connected to the Internet, unsecured, a device can be geo-located from anywhere in the world and serve as a potential entry point for cyberattacks. For example, an attacker may be able to install malware on a smart device, then steal users’ energy or wireless quota as well as personal data on users’ laptops, all without the user even knowing. There will be more serious implications if users also keep corporate information on their smart devices. Not only do smart home devices increase the range of security...
risks by increasing the potential attack surface but they also greatly increase the areas of damage if a breach does occur. For example, if a smart refrigerator is not designed properly with security, a hacker can break in, cut its power source, damage its key parts, infect it with ransomware, take control of the home network, and break down not only the refrigerator but also potentially every device on the same network that the refrigerator is on.

**Shape and Size:** The shape and size of everyday objects have evolved over decades to the point where they can best serve their pre-determined functional roles and place of deployment. The smart home products need to maintain the shape and size of their conventional counterparts. As a result, embedded components need to be small enough to fit in the everyday objects. Since smart products, unlike traditional products, require energy to sustain their continued functions, energy self-efficiency is a necessity for smart home devices. Since computational power is determined by the number of transistors on a microcontroller or a microprocessor and energy storage is also determined by size, miniaturization in hardware building blocks puts a limit on energy capacity and concurrently and subsequently computational capacity in smart home devices as well. Consequently, today’s smart home devices have insufficient processing capacities to make many popular computationally intensive features such as voice recognition work. This current technical limitation explains smart products’ dependencies on cloud infrastructures as the computational power in the cloud has much greater scalability. The problem is that connecting the everyday object to the Internet significantly expands the system boundary of the everyday object and thus adds many complexities. As a result, product security needs to include a spectrum of new system elements: hardware, software, network, associated platform and cloud infrastructure because each of these elements can be a potential entry point for cyberattacks.

**Low Cost:** It’s commercially unviable to require consumers to buy a smart lightbulb for hundreds of dollars when unconnected lightbulbs cost under $10. Since adding more processing power, memory storage, battery, software, hardware, network, platform, and cloud security all add cost (Simon & Watson, 2015), the majority of the smart home developers think that they simply won’t be able to sell products that would include all the security measures at the price point that the market would accept today. While enterprise customers are typically willing to pay for the most secure IoT products in the market to guarantee the safety of their data, consumers don’t yet have strong reasons to pay $100 extra to ensure a smart lightbulb has security. Consequently, many smart home developers seek to deliver the minimum required functionalities at the lowest possible cost. Many smart home products have simple functionalities such as gathering usage data, turning something on/off, sending/receiving information with a hub or applications that control the device. Because the tasks are simple, a lot of smart home devices use the 8-bit microcontrollers with the absolute minimum necessary memory and disk space,
which leave no room for security measures such as SSL encryption. (Simon & Watson, 2015) As a consequence, many smart home products come with no security measures whatsoever, which makes them vulnerable to interception and unauthorized access.

**Long Life**: Unlike conventional digital categories such as laptops and smartphones that are often obsolete after a few years, many everyday objects are made to be left in place for years if not decades as seen in Figure 5-1. Hence, their smart counterparts are also expected to be long-lived and always available.

<table>
<thead>
<tr>
<th>Application</th>
<th>Lifecycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy networks</td>
<td>15-50 years</td>
</tr>
<tr>
<td>Roads</td>
<td>30 years (10 years maintenance)</td>
</tr>
<tr>
<td>Vehicles</td>
<td>15 years</td>
</tr>
<tr>
<td>Home appliances</td>
<td>10 years</td>
</tr>
<tr>
<td>Lighting</td>
<td>2,500 hours for incandescent light bulbs and 25,000 for LED. (2 years to 20 years)</td>
</tr>
<tr>
<td>Consumer electronics</td>
<td>2-10 years</td>
</tr>
<tr>
<td>Telecom networks</td>
<td>10-50 years</td>
</tr>
</tbody>
</table>

**Figure 5-1: Existing Expectations for Device Lifecycle (OECD, 2013)**

Examples are smart meters and smart locks. Because these devices have long life, attackers will have plenty of time to find vulnerabilities as new threats emerge during a product’s lifetime. In particular, the hardware part of many long lasting smart things can’t be easily or cost-effectively upgraded. Therefore, ideally, the manufacturer needs to find fixes for newly exposed security flaws, and users also need to keep up with the latest patches and fixes constantly and promptly. Fixes are relatively easy to do with software, but not so with hardware. Also, hard disk manufacturers typically do not cryptographically sign the firmware the way software vendors do, nor do they make their hardware authenticate signed firmware. Consequently, the hardware is especially vulnerable to hacking. Once someone compromises the hardware and installs malware on it, the hardware can fail at random times or stop working altogether, or it can be turned into a hidden spy to steal user data without the user ever knowing it. (Zetter, 2015) Moreover, devices may outlive their manufacturers or their willingness to support, in which case, the devices will stop getting security updates and be left dysfunctional (Hern, 2016) or vulnerable to hackers if users do not uninstall punctually. In the similar vein, devices which capture data of the utmost private nature might also outlive their users when a home is transitioned from renters to renters or from owners to owners, potentially leaving the previous occupants’ data vulnerable to exploitation. Moreover, unlike smart TVs or smart lightbulbs, some devices such as the smart meters or smart locks can’t be so easily uninstalled or replaced if they are compromised. This problem makes immediate remediation difficult in some cases and potentially extends the time when the entire network is left open for exploitation.
5.2.2 System Vulnerabilities

5.2.2.1 Characteristics of the Smart Home Market and Their Security Implications

*Emerging Market:* Due to the rapid performance improvement and cost reduction in computing as discussed in Section 2.4, hardware building blocks with limited processing power such as Arduino and Raspberry Pi microcontrollers that are meant for teaching basic computer science in schools and developing countries have become widely accessible and popular for launching IoT startups. In early 2015, a microcontroller cost merely $20 (Simon & Watson, 2015). Barely half a year later, the price dropped to nearly zero (Rundle, 2015). The rapid price decline in the open-source hardware market is causing price pressure on the overall hardware market. In addition, there are plenty of free tutorials and sample code online as well as many beginner-friendly development environments to choose. The accessibility of the off-the-shelf components, devices, tools and tutorials made it commercially viable for innovators to venture into the IoT and create smart home products that are affordable enough to compete with inexpensive and durable conventional products in millions of households. Moreover, accessibility to hardware and tools also lowered the barriers to entry for innovators without formal software development experience and knowledge and skills in cybersecurity. (Simon & Watson, 2015)

According to VisionMobile, a research company in the app economy, as of late 2015, there were 1.5 million developers (32% of all IoT developers) working on smart home solutions, and 70% of them were hobbyists (Schuermans, 2015), meaning there were approximately 450,000 professional smart home developers at that time. Since little expertise is required to build and ship products, the result is a rapid proliferation of unsecured smart home products on the market. Many devices use common components and firmware that inherit all the vulnerabilities in their building blocks. For most developers, security in the components is simply assumed as they focus on how to connect the devices and how to generate valuable outcomes from the data collected. Consequently, devices that may never have been security tested were built and sold on crowd-funding sites and found their way to early adopters' homes. (Simon & Watson, 2015) Never before has the problem been laid so bare; without proper configuration and timely patches on a regular basis, known vulnerabilities in these building blocks, both hardware and software, can make device users widely exposed to cyberattacks.

*Hardware as a One-time Shot:* In a blog post published by Matt Turck, the managing director of First Mark, a venture capital (VC) firm in New York City, he explained that IoT products are, first and foremost, hardware products. He noted one of the key lessons learned from the past 2 or 3 years by IoT entrepreneurs and VCs was that building a great hardware product is a very unforgiving process and takes a very long time because hardware development can't iterate as fast as with
software development. Additionally, for hardware products, there was no such thing as a hardware Minimum Viable Product (MVP). Once a product was in manufacturing, any mistake in design would require a rework that can delay the product release for up to several additional months. (Turck, 2016) What this means is that rushed smart home products with hardware flaws often can only be fixed with manual changes or sometimes a product recall like in the case of Quirky’s Wink smart hub system (Jacobson, 2015). Addressing security issues after a product has been or is about to be released is the most expensive point to correct a problem. A similar gaffe happened to the SimpliSafe smart lock mentioned earlier. The product can’t be upgraded to defend hack attacks because it installed a one-time programmable chip. (Fox-Brewster, 2016) Stories like this that affect many customers have a huge negative impact on startups trying to build brand equity and consumer confidence.

Time-to-market Pressure: According to a recent article, the smart home market was among the fastest growing venture segments; there has been an estimated $550 million already invested in smart home technologies up to this point (Herceg, 2016). In a recent survey by Autho, a company that offers single sign-on services, 85% of developers confessed that they felt rushed to get an application to market due to demand and pressure within the previous six months, and 90% of developers believed that current IoT devices do not contain the necessary security as shown in Figure 5-2 (Flittner, 2015). The time-to-market pressure is a typical characteristic of startups operating in an early market (Turck, 2016) because many entrepreneurs need to demonstrate value to existing and future investors and speed-to-market is key to gain investors’ confidence. The increase in the smart home exhibitors at CES of the past two years is a clear indicator of how rapidly the smart home products become available on the market. There were 60 smart home product exhibitors at CES 2015, and this number grew to 156 at CES 2016. Although the time-to-market strategy may work out fine for many Internet startups, it is dangerous for the smart home startups because, precisely as mentioned, smart home devices are not software products but first and foremost hardware products. They should have the same security measures as other hardware devices such as laptops. For developers in a rapidly expanding, intensely competitive market where time-to-market is critical so as not to get left behind, security unfortunately often come as the last priority if it’s on the priority list at all.
Startup developers are facing many challenges. Due to resource constraint, the complexity of the home environment and the lack of an established customer base, a typical startup will have a hard time to find the resources to build a platform for an entire house. Instead, most innovative smart home startups focus on delivering one specific product. For example, Hydrao is a smart showerhead that teaches you how to save water indoors (Ulanoff, 2016). The result is a highly fragmented, diverse and crowded market. Moreover, each smart home product brings with it an ecosystem of multiple suppliers/partners. The dependencies of startups on external collaborators further exacerbate the complexity in the smart home environment since these devices and their suppliers/partners can have very different security policies. As can be seen, the current fragmentation and complexity in the smart home market make the security of the smart home system very difficult if not a completely elusive idea.

**App Economy vs. Device Economy:** Because the smart home market is still nascent, many companies have yet to figure out what platform models and business models would work best for this market. One thing that is sure is that the device economy will be different from that of the app economy. Unlike apps, devices are hard to install, upgrade and remove and are expected to work for a long time. The application model that fueled the success of smartphones will probably not work for the smart home.

5.2.2.2 **Characteristics of the Smart Home and Their Security Implications**

**Automation:** The ultimate vision of the smart home is to have devices entwine with the physical world, collect and understand information and collaboratively coordinate tasks and make decisions on users' behalf with little intervention or even
user awareness necessary. Smart home products instigate more user benefits than conventional products because smart products allow users to share their personal data without effortful and intentional inputs since data analyzed collectively (data of the same type from every person in the same household) and across time (data of the same type from one person for the past year) are more valuable than a single data point. The smarter a system's automation, the more benefits the smart home will produce for its users. The problem is, as with many complex systems, individually vulnerable components when combined create further vulnerabilities that are often hard to predict. In particular, the smart home's reliance, to some degree, on intelligent coordination means data integrity is of critical importance because faulty data can lead to incorrect state estimation, which can mislead devices and sometimes their owners into making potentially catastrophic decisions. Data integrity for the entire home coordination network requires data integrity for each device because a compromised smart device will open the entire network of devices to be attacked as well. Moreover, automation and connectivity also add new dimensions of trade-offs and challenges such as scalability, availability, portability and usability to smart product manufacturers, which further increase the complexity in the home environment and contribute to making the home less secure.

A Shared, Private, and Highly-customizable Environment: Unlike cities or buildings, the home is, first and foremost, the most private habitat which locks within a treasure trove of sensitive personal data and a much smaller and thus more concentrated target where everyone with physical access can easily locate most of the smart devices in a home. Unlike health, which is per individual basis, home is surely in most situations a shared resource with multiple occupants where at least the head of the household would need complete control and assurance of its safety, security and privacy. Unlike cars, where all the components and how they integrate together have limited degrees of freedom because of a common design, homes can vary widely and are highly customizable places with a hard to predict dynamic context. Unlike traditional digital devices such as laptops and smartphones, where a hacked device can cause data or financial loss or other nuisances, a hacked smart home device such as an air conditioner locked by ransomware in the middle of a broiling summer can lead to personal harm and even death. Furthermore, data sharing of the most personal nature and of various granularities that might require users’ consent add further complexity to the home environment. All in all, these essential qualities of the home generate a great level of complexity and hence a unique combined set of security challenges that none of the other IoT domains have. Furthermore, as an example, the level of access privilege for each smart device should differs from the householders to their kids to their parents and grandparents to visitors to service workers such as babysitters and renovation/repair/painting helpers to unauthorized intruders; each has a different set of preferences/judgment and technical/security sophistication. None of this complexity was problematic
until the “things” started to connect to the Internet and talk with each other, and many current smart devices made the simplified assumption that they can trust everyone in the home with everything. Together, the interconnectedness and security being unchecked allow an attacker to potentially gain access to every device in the home network, turning the home into a security nightmare.

**Heterogeneity & Multiplicity:** The Organization for Economic Co-operation and Development (OECD) estimated in 2012 that a four-person family with teenagers may have around ten connected devices, and this number will increase to 50 per household in 2022 (Figure 5-3) (OECD, 2013).

<table>
<thead>
<tr>
<th>Device Type</th>
<th>2012</th>
<th>2017</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 smartphones</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2 laptops/computers</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 printer/scanner</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 game console</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 DSL/Cable/Fibre/Wifi Modem</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1 eReaders</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 smart metre</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2 connected stereo systems</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 Internet connected car</td>
<td>1</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>1 pair of connected sport shoes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 pay as you drive device</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>1 network attached storage</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 digital camera</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>1 energy consumption display</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 energy consumption display</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 connected set-top boxes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3 connected set-top boxes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 connected television</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 printer/scanner</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 game console</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 smart metre</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 Internet connected car</td>
<td>1</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>1 pair of connected sport shoes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 pay as you drive device</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>1 network attached storage</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 printer/scanner</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 smart metre</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 energy consumption display</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 energy consumption display</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 connected set-top boxes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3 connected set-top boxes</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 connected television</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1 printer/scanner</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

**Figure 5-3: Number of Smart Devices in a Household of Four (OECD, 2013)**

The smart devices are heterogeneous in types, ranging from smart lightbulbs to smart TVs to smart thermostats and meters, but also, there could be a motley of devices of the same type (multiplicity): for example, different lighting installations in different rooms. The amounts of heterogeneity and multiplicity of connected devices are smaller in a home environment than in cities or buildings, but these characteristics still make the home environment much more complex than it ever was due to the following reasons. First, each device has a different set of use scenarios. For example, a smart thermostat learns occupancy and consumer preferences and adjusts the indoor temperature accordingly whereas a smart alarm
allows users to be alerted upon an intrusion and gives users peace of mind. What this means is that the potential number of the paths of interactions could be large. Diversity in the paths of interactions increases the attack surface by increasing the complexity in timing considerations of device-to-device communications and opens more venues for successful breaches. Secondly, devices do not all have synced lifecycles. For example, the lifecycle of a smart thermostat which is typically expected to last for decades is different from that of some smart lightbulbs which normally only last for a few years (Figure 5-1). As a consequence, the timing needed for software and hardware updates are different from device to device. Because ensuring up-to-date information on all devices is such a cumbersome task for users, this increases the chance of outdated devices being left on a home network, and therefore, increases the chance of attacks.

**Multiple Control Access Points:** One of the key features of many current smart home products is that they are controllable through a mobile device such as a smartphone. The remote access also allows tech services to perform diagnosis and provide resolution more effectively and efficiently. However, these added benefits open new risk vectors. First of all, mobile devices such as smartphones could be themselves vulnerable when they get stolen or lost or when the devices are left alone unprotected, which in turn could give wrongdoers an easy way to access the control of the victim’s smart home. Now, compounding this risk is the proliferation of new control access points that will increasingly make the detection of intrusions and breaches more complex. For example, Ford is working on pairing millions of connected cars globally with smart home devices that allow users to control home functions such as lights, entertainment, garage doors and even home security systems (Ford, 2016). Vinli, a startup company, developed a Vinli Home Connect platform that was compatible with Icontrol Networks, Google’s Nest and Samsung’s SmartThings and allowed users to integrate their smart home with their smart cars (Takahashi, 2016). While these innovations may increase convenience for users, they also obfuscate the system boundary of the home more and more. The result is that it not only becomes increasingly more challenging to keep a clear view of whether data flow from one system to another is trustworthy or not and where attacks or breaches occur when they do occur, but it also increases the potential spread of damage when breaches do happen.

**Human Origin:** In the Autho survey mentioned earlier, only 18% of the consumers surveyed trusted having their personal data tied to IoT devices (Flittner, 2015). Although there is a definite acknowledgment of mistrust in IoT devices, most consumers aren’t aware how security breaches occur and also lack the capabilities to protect themselves. Nor are they cognizant of which devices have poor cybersecurity and which are relatively more secure. Besides, the majority of the people have not personally experienced cyber breaches or had their computers infected with malware. Many of the products such as smart lightbulbs, where
security was never a concern before, appear completely harmless. Many early adopters also can't think of why anyone would want to target their home nor are they aware how smart home devices could expose their network to hackers even if nobody targets them specifically. Furthermore, unlike connected cars, the meaning of cybersecurity in the home context is relatively less well understood by everyone. On the organizational side, corporate boards, for example, are yet to realize how smart products will impact their organization and even less how the smart products in their employees' home could be taken advantage of to make inroads into enterprise data and networks. According to Gartner Inc., a research firm, as of 2015, the “budgets for IoT security contributing on average less than 1% of global budgets for cybersecurity” (Friedman et al., 2015). On the consumer side, because each smart home product is from a different vendor, consumers and amateurs are left as the integrators of the smart home. On the legal side, due to several large enterprise breaches in the previous years, in 2015, governments all around the world hastened to introduce corporate cybersecurity regulations (Ahmed et al., 2015). However, regulations in the smart home market are yet to catch up with the speed of development of the smart home products. In the health IT world, for example, physical harm and liability caused by hacked medical devices top cybersecurity fears for leaders (Dvorak, 2016). While the smart home products can potentially engender consequences potentially more severe, they don't seem to scare smart home innovators as much. Finally, engineering today’s complex technology products in the commercial setting often requires an interdisciplinary approach as skill sets normally do not overlap much. The main reason is perhaps because engineers tend to focus on developing specific skill one at a time. For example, product engineers and designers that are good at design and creating new devices normally are not interested in or good at breaking products. The bottom line is that building great smart home products, given all the constraints one has, really is not as trivial as many innovators might think. It requires a cross-disciplinary effort and skill set that many startups lack.

5.2.3 Product vs. System Security

A paper published by Colonel William Young, a then-PhD student at MIT’s Engineering System Division, and Professor Leveson in 2014 pointed out that security like safety was an emergent system property because only the context of the system security viewed holistically could determine security. The paper went on saying, “Hazards lead to safety incidents in the same way that vulnerabilities lead to security incidents ... the key question facing security analysts should be how to control vulnerabilities, not how to avoid threats.” (Young & Leveson, 2014) As a result, securing individual smart home products including hardware, software, platform, and cloud infrastructure won't be enough. Even if every single smart device is secured individually, the smart home as a whole could still be insecure. At the 2016 STAMP (System-Theoretic Accident Model and Processes) workshop,
Colonel Young said that systems that were not designed to be secure in the first place might not be possible to secure at a later time. In Professor Nancy Leveson's 2012 book referenced in Chapter 1, she concluded that almost all the serious software accidents in the past twenty years were not caused by coding errors but due to requirements flaws. She said “The requirements may reflect incomplete or wrong assumptions [1] About the operation of the system components being controlled by the software ... or [2] About the required operation of the computer itself.” (Leveson, 2012) As explained in the previous sections, cybersecurity is not currently a requirement for many smart home products. Additionally, cybersecurity is also not a requirement for the smart home system because it's not yet being viewed as a system. Based on the evidence provided in this section, the smart home system, with the way it's getting developed now, cannot be secured in the future.

5.3 Causal Loop Diagram

Figure 5-4 includes the new dynamics detailed in this chapter.
The new variables are “Attractiveness of the Smart Home to Attackers,” “Vulnerabilities in the Smart Home” and “Complexity in the Smart Home.” Two new loops are added are R5, “Complexity Begets Vulnerabilities,” and R6, “Vulnerabilities Begets Attacks.” All new additions are highlighted in orange. R5 explains the particular feedback when the increasing time-to-market pressure increases the complexity in the smart home, in turn making the smart home more vulnerable due to a plethora of unsecured devices rushing into the market. R6 explains the dynamics that the increasing vulnerabilities of the smart home will increase their attractiveness to cyber attackers because of the relative ease with which the smart home can be compromised.
6 Values at Risk

“You must take your place in the Circle of Life.”

- Lion King

6.1 Value the Missing Link

So why aren’t there any major breaches by cybercriminals in the smart home yet? Simply, it’s because the smart home has not yet been successful with the mass market; there is not much value to be gained by hacking into a few early adopters’ homes. Chris Babel, the CEO of the data privacy management company TrustE, explained, “Everything is still very siloed, and it’s not very connected.” He went on saying that there would be massive amounts of value, from both the users’ and the hackers’ perspective, when everything gets connected. (Wood, 2015) According to an email interview conducted by eweek.com with Symantec researchers, there haven’t been any active exploitations in the wild even though plenty of vulnerabilities do exist. They added that once hackers found motivations, these devices would be inevitably targeted and broken into in the near future unless manufacturers proactively implement necessary security measures. (Lemos, 2015) In other words, if there are enough incentives to motivate cybercriminals to want to attack the smart home, they will. Currently, there are other more valuable targets on hackers’ priority list to break. When market leaders emerge and their ecosystems become more mainstream, and as more devices gain access to users’ financial data and personal information such as health records, these devices will attract more attacks as the potential economic gain increases for the attackers when more users are affected.

The following sections clarify the values at risk in more detail by exploring these values both from the device manufacturers’ perspective and the industry’s perspective.

6.2 Risk Implications to Smart Home Device Manufacturers

“Good judgment comes from experience. Experience comes from bad judgment.”

- Jim Horning
6.2.1 Market Growth Risk Implications

In late 2015, Venturescanner.com reported that IoT Home is the IoT category that had seen the most innovations (more than 140 startups developing the smart home solution) as well as the most venture investment (more than $1.2 billion invested) (Figure 6-1) (Venture Scanner, 2015).

![Venture Investing in IoT by Venture Scanner](image)

**Figure 6-1: Number of Startups and Amount of Venture Invested for Each IoT Category (Venture Scanner, 2015)**

Various forecasts predicted that the smart home market will be in the range of tens of billions of dollars in the US and hundreds of billions globally by 2020. However, despite the promising predictions and a huge amount of interest in the startup scene, numerous studies showed that consumers are hesitant to use the technology. A survey result released by Coldwell Banker Real Estate LLC in early 2016 indicated that there was still real consumer interest in the smart home technology, but consumers were concerned about security issues. Elizabeth Cholawsky, the CEO of Support.com (a company that specializes in providing technical support for products), in a separate interview, also said that “they will buy it when security and safety issues are worked out.” (Clark, 2016) Another survey by Parks Associates, a research firm, reported that 47% of US broadband households were concerned about privacy or security of smart home devices. Tom Kerber, the Director at Parks Associates, explained that the recent high-profile media coverage of hacked smart
baby monitors and connected cars had raised consumer concerns about privacy and security issues of the smart home devices. He went on saying that companies needed to take these concerns seriously and move quickly to reinforce the security and privacy of their solutions. (Parks Associates, 2015) In the same consumer survey mentioned in Chapter 3, Accenture concluded that the recent adoption of the IoT had been much slower than expected and not enough to fill the gap left by the stalling of the traditional device market. The top three reasons for the stalling growth of the IoT, in order of consumer priority, are 1) lack of compelling value proposition, 2) security concerns and 3) price. Among these three issues, consumer awareness of security concerns has become a top barrier. In that survey, a majority of consumers was aware of some of the recent, extensively publicized cyber breaches. As a result, among these consumers, 42% had decided to either postpone IoT purchases or terminate their existing devices and services. For consumers, risks had outweighed previously perceived value in purchasing decisions. (Accenture, 2016) Following these concerns and many issues surrounding the smart home products such as usability and price, the smart home market is currently stuck in the “chasm” on the technology adoption curve as illustrated in a BusinessInsider.com article (Greenough, 2015).

What all these statistics seem to suggest is that the security of smart home products is a critical success factor for product adoption. Without security assurance in place, it is unlikely that the IoT will be able to successfully innovate into the most private and personalized space of the home.

6.2.2 Liability Risk Implications

6.2.2.1 Case 1: Users’ Workplace

Many hacking examples in the previous chapter showed that insecurity in the smart home devices can be taken advantage of by cybercriminals to break into users’ home network and launch attacks against anything connected to the same network such as tablets, phones, and computers. Moreover, some of these devices may move subsequently into corporate networks, thereby extending the risk of attacks into the enterprise. According to a recent article by Michelle Drolet, there were increased cyber incidents that targeted high-level execs or anyone with a high-security clearance specifically, because breaking into a CEO’s account would allow cybercriminals to expose a lot of sensitive data and hence be much more valuable (Drolet, 2015). Many high-level executives are tech-savvy and also typically interested in and can afford expensive gadgets to furnish their home. For example, a former Apple executive has a $35 million California mansion with connected lighting, music, TV, air conditioning, window blinds, fireplace and door locks that are all controllable through iPhone or iPad (Dormehl, 2015). From an attacker’s perspective, hacking access credentials of superusers to access corporate and government networks and databases makes far more financial sense than say
hacking just anyone. Moreover, many smart home products such as smart bottle hydration systems are just as mobile as smartphones and wearables. And needless to say, companies cannot prevent their employees from purchasing and installing unsecured consumer-grade smart home products and cloud services in their home nor can they stop employees from bringing their smart products to work and connecting them to the corporate network. Indeed, according to McKinsey, today’s organizations are expected to be more “open” than ever before as employees start demanding access to corporate networks through their personal mobile devices (Kaplan et al., 2011). This phenomenon is often referred to as the “bring your own device (BYOD).” BYOD already has made controlling the movement of sensitive documents very challenging for workplaces. New mobile smart products will further aggravate the situation as they become increasingly more common. In its 2015 Internet Security Threat Report, Symantec said, attackers continued to try various attacks on targeted corporate networks from different angles to gain unauthorized access. Often, they looked for weaknesses in companies’ defenses to exploit whatever vulnerabilities they can find. For example, they can attack the perimeter of the network as showed in many attack cases in 2014. Determined attackers frequently attack a target company’s supply chain as a way to outflank its security. (Symantec, 2015) Notably, Employees are part of a company’s supply chain, and the smart products will expand the enterprise threat surface by opening many easy inroads for hackers and many more opportunities for potential breaches. Additionally, as can be seen in many recent corporate breaches, depending on the type of industry and how sensitive the data involved are, risk impacts to enterprises alone would include intellectual property loss, financial loss, customer defection, market share loss, brand erosion, privacy and competitive breach, etc. Furthermore, there would be peripheral damage on ecosystem partners and suppliers. In fact, Gartner predicted that by 2020, addressing compromises in IoT security alone would rise from less than 1% of corporate annual security budget in 2015 to 20% (Rossi, 2016).

6.2.2.2 Case 2: Smart Grid

As seen in the cases of the spamming refrigerator and the whole building botnets, every poorly secured Internet-connected smart device does not have isolated effects locally, but rather can affect the security of the Internet globally. In particular, the smart grid, which has been deployed widely and played a vital role in integrating various clean, renewable energy solutions, modernizing the electrical system to increase performance, reduce carbon footprint and save energy and cost for end consumers. Due to its critical role and wide-reaching characteristic, the smart grid is an attractive target for cyberattacks. And as mentioned in the last chapter, smart meters are what connect millions of households to the smart grid. Through the smart meters, the smart homes become the edge nodes of a smart grid. And once connected to the smart grid, any smart home can potentially interact with any other smart home on the grid in an authorized or unauthorized way; therefore, a breach
in the smart home can potentially compromise the security of an entire grid. In the most severe case, a breach in data integrity or a malicious change in meter measurement can black out the energy supply of a house or an entire neighborhood. Other perhaps less dangerous consequences include energy thefts and pricing hacks.

6.2.2.3 Previous Lawsuits

In the past three years, there have been a number of lawsuits filed against device companies, mostly by the Federal Trade Commission (FTC), the primary government agency in the US for consumer protection. According to an article published in 2015 on insidecounsel.com, a magazine specifically designed to serve general counsels and other corporate legal professionals, the earliest prequel policing efforts traced back to 2013. In 2013, the FTC sued HTC America on the allegation that HTC misrepresented in its privacy and security policy the security vulnerabilities in the apps pre-installed on its smartphones that “could allow third parties unauthorized access to user data and device functionality.” In the ensuing settlement, HTC was not only required to “patch affected devices, develop a comprehensive security program” but also to be audited biennially for 20 years. Following in 2014 was the FTC’s first charge against an IoT company, TRENDnet Inc., which, as described in the last chapter, had advertised its insecure Internet camera for secure remote monitoring. In 2012, the hacked TRENDnet’s cameras leaked hundreds of users’ videos, all posted online for public viewing. The FTC’s settlement terms with TRENDnet were similar to that for HTC. (Kleine et al., 2015) In 2016, FTC brought another action, this time, against Asus Wireless due to many insecurity issues in its wireless routers such as default username and password, easily hackable admin panel, etc. in its routers that were advertised as secure. The settlement the FTC had with Asus Wireless in 2014 also included a requirement for independent security audits biennially for the next 20 years. Moreover, Asus was required to pay a civil penalty of up to $16,000 for each additional violation. Barely a month later, researchers found that the same security issues affected Asus routers in 300,000 routers manufactured by D-Link, Micronet, Tenda, TP-Link, and others as well. (Krishnan, 2016)

The FTC is not the only stakeholder that has brought legal actions against device makers. A report by US Senator Edward Markey in February 2015 has spurred the first IoT class action brought by a Dallas law firm against three major international automakers Toyota, Ford and General Motors in 2015. The lawsuit was based on the several theoretical hacking scenarios that were demonstrated at events such as the Black Hat security conference in 2014. (Mearian, 2015) In a similar case of lawsuit brought by Helene Cahen of Berkeley, California, also in 2015, she complained about her 2008 Lexus RX 400 H. Although the car had not caused her any bodily harm or failed to function as advertised, she argued that, in theory, the car could be remotely
hijacked to cause personal injury based on various existing literature on hacking examples of cars’ wireless component. (Fisher, 2015)

As the smart home and IoT market just start to emerge, it is often unclear to the smart home manufacturers who would be liable if a cyber breach does occur. But as can be seen in the above cases, often, the device manufacturers are the ones that are responsible and are the targets of direct litigation. Although these legal cases are all filed against large IoT manufacturers, it is important for the smart home startups to realize that there is a mindset shift occurring now where government entities, law firms and consumers can all sue device manufacturers for security issues that can lead to personal injury and property damage.

6.3 Risk Implications to the IoT Industry

“Trust takes years to build, seconds to break and forever to repair.”

- Unknown

6.3.1 Value of IoT

First of all, to understand the impact of cybersecurity of the smart home on the IoT more broadly, it is helpful to understand the current IoT values at stake first.

The “father of sensors,” Janus Bryzek, predicted IoT to be the “largest growth in the history of humans.” Many research firms and tech incumbents have made IoT projections in the past few years. According to the research firm IDC Corp., in 2014 alone, 10.3 billion devices had already been installed; the total installed base of IoT endpoints would be 29.5 billion in 2020, and the expected total of Internet-connected devices would total 200 billion by 2020 (Press, 2015). Additionally, the IoT is not just a volume market, but also has huge economic impact. The global IoT market was forecasted by IDC to burgeon from nearly $2 trillion in 2013 to $7 trillion in 2020 (Wood, 2015). McKinsey estimated the potential economic impact of the IoT in 2025 to be $3.9 trillion to $11.1 trillion per year (Manyika et al., 2015). To put this into perspective, the worldwide smartphone market was estimated to be $50 billion to $450 billion per year from the year 2009 to 2018, an order of magnitude lower (Kenie, 2015). In 2014, IDC predicted, within the next five years, all industries will have implemented IoT initiatives specific to their needs (IDC Research Inc., 2014). As the worldwide investment in the IoT has already been accelerating. GE predicted that the IoT could benefit as much as half of the global economy (NIST, 2015).

Many cities such as Barcelona and Singapore are undergoing transformation into smart cities where the management of city services like parking, trash collection, and traffic lights are all started to be automated (Wellers, 2015). In particular, Singapore has aimed to become the world’s first smart nation through its Smart
Nation Program started in 2014. The program has instituted a wide range of initiatives that apply the smart technologies in areas such as infrastructure, green/smart buildings, public transport/traffic management, environmental sensor networks, smart energy grids and meters, smart homes, telehealth to “improve quality of life, create more economic opportunities, and support stronger communities.” (Jakhanwal, 2015)

Many large companies that invested in the IoT early on had harvested well from their investment. For example, in 2013, Intel’s IoT group generated $1.8 billion in sales and $550 million in operating income, comparable to the operating profit of ARM Holding’s entire business in the same year (Eassa, 2014). In 2014, Verizon saw a 45% year-after-year revenue growth; the majority of this growth came from the adoption of IoT in the manufacturing sector (204%), finance and insurance sector (128%), media and entertainment sector (120%), home monitoring sector (89%), retail and hospitality sector (88%), transportation and distribution sector (83%), energy and utilities sector (49%) (Berg, 2015). As a result, additional investment has been pouring in. In early 2015, IBM announced it would invest $3 billion over a four-year span into a new IoT business unit (Rigby, 2015). Alphabet/Google has invested billions in the IoT (Nest for smart home, SideWalk Labs for smart cities, etc.). Intel, Qualcomm, and ARM have been competing to dominate the IoT chip market. In February 2016, Cisco acquired IoT platform provider Jasper for $1.4 billion (Cisco, 2016). AT&T has been working on connectivity for cars through partnerships with nearly all major US car manufacturers (Mccracken, 2015).

On the startup scene, the blog post published by Matt Turck as mentioned in Section 5.2.2.1 also attached a one-picture view of all the IoT startups involved in the early 2016 IoT landscape. This chart was produced by his firm First Mark. (Appendix F) As can be seen at a glance, hundreds of startups are current working in this space.

Furthermore, IoT does not only have substantial business values but will also play a crucial role in job creation, especially to address the current skyrocketing global youth unemployment rate, as touted in a post published on Cisco Blogs in September 2015 by the Senior Vice President Tae Yoo. She said, “Ultimately, if we can harness the power of the rocketing IoT global phenomenon and align some education, curriculum, and learning to the technology job market, we can use it to fuel economic growth.” She added that “Cisco believes [IoE’s] impact on society will be [5] to 10 times greater than the impact of the Internet to date. The post also mentioned that, according to Vision Mobile, there will be 4.5 million entrepreneurs, innovators, and developers working on projects related to IoE by 2020.” (Yoo, 2015)

6.3.2 Word-of-mouth

“When people are free to do as they please, they usually imitate each other.”
As much as the smart home is a highly complex application environment for the IoT as explained in Section 5.2.2.2, it should be, at least in terms of the interoperability requirement, less complex than many other IoT application environments. In fact, the same McKinsey research mentioned earlier estimated that interoperability should be required for about only 17% of the potential value in the home setting, the lowest among all IoT applications and much lower than the average interoperability requirement of 40% of potential value across all IoT domains (Figure 6-2) (Manyika et al., 2015).

**Exhibit 2**

*Nearly 40 percent of economic impact requires interoperability between IoT systems*

<table>
<thead>
<tr>
<th>Potential economic impact of IoT</th>
<th>Value potential requiring interoperability</th>
<th>% of total value</th>
<th>Examples of how interoperability enhances value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$11.1 trillion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38%</td>
<td>1.3</td>
<td>36</td>
<td>Data from different types of equipment used to improve line efficiency</td>
</tr>
<tr>
<td>62%</td>
<td>0.7</td>
<td>43</td>
<td>Video, cellphone data, and vehicle sensors to monitor traffic and optimize flow</td>
</tr>
<tr>
<td></td>
<td>0.7</td>
<td>57</td>
<td>Payment and item detection system linked for automatic checkout</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>56</td>
<td>Linking worker and machinery location data to avoid accidents, exposure to chemicals</td>
</tr>
<tr>
<td></td>
<td>0.4</td>
<td>44</td>
<td>Equipment usage data for insurance underwriting, maintenance, pre-sales analytics</td>
</tr>
<tr>
<td></td>
<td>0.3</td>
<td>20</td>
<td>Multiple sensor systems used to improve farm management</td>
</tr>
<tr>
<td></td>
<td>0.3</td>
<td>29</td>
<td>Connected navigation between vehicles and between vehicles and GPS/traffic control</td>
</tr>
<tr>
<td></td>
<td>0.1</td>
<td>17</td>
<td>Linking chore automation to security and energy system to time usage</td>
</tr>
<tr>
<td></td>
<td>0²</td>
<td>30</td>
<td>Data from different building systems and other buildings used to improve security</td>
</tr>
</tbody>
</table>

1 Includes sized applications only, includes consumer surplus.
2 Less than $100 billion.

NOTE: Numbers may not sum due to rounding.

SOURCE: Expert interviews; McKinsey Global Institute analysis.

**Figure 6-2:** Interoperability’s Impact on the Total Economic Value for Various IoT Domains (Manyika et al., 2015)
What this translates to is that even though the smart home innovation scene is plagued with security problems, it should be a relatively easier environment to connect devices than most other IoT settings because it is more contained, less dynamic, with limited valuable connections compared to, for example, the industrial IoT. With industrial IoT such as the smart cities, cargo tracking, and precision farming, there needs to be a mass-scale deployment of homogenous IoT devices. For example, as of early 2016, the largest industrial IoT network deployment in the US is by Sigfox, a French networking company, that has already been supporting several large IoT network stations in Europe. Sigfox is in the process of expanding its IoT deployments to ten US cities by the end of the first quarter of 2016. Sigfox’s technology comprises Low-Power Wide Area Networks (LPWAN) and hardware components that connect any device to the Internet with ultra-energy efficiency (“go to sleep” when not in use). (Neagle, 2016)

Moreover, one key characteristic for the general IoT adoption is the pervasiveness of intelligent embedded “things” that users need to trust to work flawlessly together in the background without much human supervision. Another key characteristic for the general IoT adoption, similar to many other high-tech industries, is the word of mouth (WOM), the process through which information spreads through people talking with each other. There are many ways to lose users’ trust; one such way is through negative WOM. As demonstrated in Section 6.2.1, negative WOM has already reduced trust in the the smart home products. Also, as illustrated in the previous chapter, negative WOM for one product/system may be compounded and multiplied by the fact that the sensors used in one smart product could be reused in many other products so a public security exposure can render simultaneously many products vulnerable at the same time. This can be seen in the case of Jeep Cherokee example described in Chapter 1, where the hack in the Jeep resulted in millions of recalls for Chrysler. Recalls in many industrial IoT settings such as in cargo tracking, which had already reached 1.8 million IoT devices deployed in total worldwide in 2014, would be devastating (Investorideas, 2015). All in all, this means that many recent high-profile breaches and hacking examples not only raised concerns and impeded the growth of the smart home market alone but also generated negative WOM for the IoT as a whole, hence further hindered large-scale deployment of IoT systems and broad customer adoption of IoT applications in other use settings. In fact, according to a survey by James Brehm & Associates, a strategic consulting firm, conducted in the early 2016 based on 108 responses from business executives worldwide, 64% of the survey’s correspondents indicated that security was a top barrier to IoT growth (Figure 6-3) (eMarketer, 2016).
Furthermore, as a result of delayed adoption, the envisioned values for IoT may never materialize or materialize in time. Researchers with Symantec's security response group said in an email interview with *eWEEK*, "It would be unfortunate if a large scale, singular incident was the turning point for IoT [industry]. These vulnerabilities are easily fixed, and with proper security methods in place, a potential disaster scenario is easily avoidable." (Lemos, 2015)

**6.3.3 Innovation Resource Allocation**

Finally, companies have limited time and energy, so if they don’t see success in the smart home market, they will reallocate their resources to somewhere else. This can be seen in the case of GE, which sold its appliance division to Sweden’s Electrolux in 2014. GE had worked on an idea of a “Net Zero Energy” home since 2009, during which time its appliance’s revenue declined nearly 18%. Natarajan Venkatakrishnan, the Director of research and development at GE Appliances, said in an interview with cnet.com that running electric dryers from roughly 250,000 homes equaled energy use of one coal plant. According to the EIA, there are over 557 coal-powered plants and nearly 3,000 natural gas and petroleum plants in the US alone. From GE’s perspective, it made perfect financial sense to shift resources from consumer IoT to industrial IoT because selling to one utility company even just for one power plant was much easier than selling to a quarter of a million consumers a technology that only provided marginal benefit to their electrical bill. Again, GE had not discovered a way to make its “Net Zero Energy” vision a profitable proposition. (Pino, 2014)
phenomenon is illustrated well in Professor Repenning's paper where he said, "If the experts believe that the innovation works particularly well in a given area, they will increase the fraction of their time and energy dedicated to that area. As they allocate more resources to area one, all else being equal, participants in that area respond by increasing their efforts. Additional effort leads to additional results and reinforces the experts' beliefs about the efficacy of the innovation in that area. These links create a positive feedback loop. This process of experts' reinforcement process equally applies to area two." (Repenning, 1999)

6.4 Causal Loop Diagram

This chapter explores how building the consumer confidence in IoT, specifically in the context of the smart home, is also critical to the success of IoT in the other domains. Figure 6-4 builds upon Figure 5-4 and Figure 1-3 with three additional loops. R7, "Other IoT Innovation Reinforcement," is a reinforcing loop that explains the fact that experts often have to choose between various options of where to best invest their resources such as time and effort. If one innovation area works out particularly well, the experts will likely to invest more resources in that area, thus reducing resources experts can invest in other innovation areas. In this specific case, the innovation area one is the smart home space and the innovation area two is other IoT innovation. The second loop, B9, "WOM," illustrates the idea that with increasing cyber breaches, negative WOM will increase as well hence reduces the trust in IoT overall. Finally, the third loop, B10, "It's All Connected," explains the dynamics that the number of cyber breach cases will also directly influence the potential number of lawsuits that will be filed against IoT, especially against the smart home device manufacturers. Both B9 and B10 reduce the value captured in other IoT innovation as well as the value captured in the smart home, which in turn, leaves the societal/consumer needs and the business pressures discussed in Chapter 3 unfulfilled. There are three key insights in this final causal loop diagram. These insights are 1) both values at risk and vulnerabilities are key to make the smart home an attractive target for cyber attackers; 2) if the innovation in the smart home is unfruitful, experts may shift their resources to invest in other IoT domains temporarily; 3) ultimately, negative WOM and lawsuits reduce the trust in the IoT devices overall, not just in the smart home devices alone, so in the long run, cyber breaches in the smart home will reduce the innovation effort in the entire IoT industry.
Figure 6-2: Final Causal Loop Diagram
7 Few Cases of Promising Technology Advancements

"The great accomplishment of men has resulted from the transmission of ideas and enthusiasm."

– Thomas Watson

Even though, as previously shown, cybersecurity vulnerabilities are mounting, some recent technology breakthroughs and frontier initiatives have promising values to the IoT innovation going forward. The following new technology development are examples of such effort. These technologies have not yet been applied or are still in the experimental phase to be applied to the IoT or the smart home.

The first example is on the infrastructure side, SRI International’s Compute Science Laboratory and University of Cambridge Computer Laboratory have a joint research project called Clean Slate Trustworthy Secure Research and Development (CTSRD). The CTSRD initiative does not aim to replace the existing Internet infrastructure, but rather to integrate “a hybrid capability model and continuous hardware-assisted validation of security design principles” into the existing hardware-software security interface thus making the Internet more secure. The CTSRD has been in existence for many years. Dr. Neumann and Dr. Shrobe, two of world’s most prominent computer security pioneers, said in an interview with The New York Times back in 2014, that CTSRD can resolve a common computer design defect, namely DoS, that allows hackers to overload a system with messages that cause it to buffer overflow, which in turn lets them install malicious code. (Perlroth, 2014)

The second example is a startup company, Lexumo, which spun off from Draper, a US defense research and development firm. Lexumo uses a novel approach to combine big data analytics and software analysis for an automated cloud-based application that can continuously monitor for known vulnerabilities in systems that incorporate open source software, and it can also pinpoint a vulnerability with high granularity and accuracy to the exact code level thus alerting users for timely remediation. (Reuters, 2016)

The third example comes from a recent research breakthrough at MIT. In a new paper published in April 2016, researchers from MIT’s CSAIL and artificial intelligence (AI) startup PatternEx showcased an AI platform called A12. This platform combines human expertise with pattern matching, and can predict cyberattacks with three times more accuracy (as much as 85% of the cyberattacks) while reducing the number of false positives five times more than any existing
methods. Moreover, this AI platform is self-learning and can improve its accuracy over time and rapidly. (Conner-Simons, 2016)

The last example is based on the blockchain, the underlining technology innovation for the bitcoin, a distributed ledger that can track and encrypt all kinds of digital exchanges securely and verifiably. The security of the blockchain increases as more people participate in it because as the number of participants increases, more computers will audit the activities, hence making it harder for attackers to undermine the system. As Dan Wellers said in a blog post, the blockchain drastically increases the cost and difficulty of collusion and subversion for attackers so that it’s simply not worth the effort of cracking. Because of the blockchain’s inherent and automatic distributed coordination and verification architecture, it is by design tamper-resistant and more secure and thus it removes the need for a separate trusted third-party. (Wellers, 2015) Several large companies are backing up the use of the blockchain technology in the IoT; most recently, a joint effort by IBM and Samsung demonstrated a proof of concept of applying blockchain to a large distributed network of IoT devices (Higgins, 2015).

Although novel advancements in security technologies such as the ones listed above are just emerging, they will continue to develop and improve to a point where they are feasible for commercial use. It’s not hard to envision at least two possible specific applications in the smart home in the future. Application one would be a system within the smart home that can automatically monitor and detect malicious activities for all devices and transactions to ensure damage is contained and remediated. Application two would be to require all devices to implement the blockchain technology, to the same effect. While none of these technologies promises to solve the cybersecurity issues 100% in the smart home and IoT by itself, perhaps together with existing standard security procedures, they can promise a future state of the smart home and IoT that is significantly more secure and more resilient than it is now. Currently, in the absence of such systems and implementations, there are many security guidelines for IoT devices such as the one from the FTC. From a long term perspective, industry leaders and major stakeholders should seek to collaborate and approach the smart home as a system, and make the cybersecurity of the smart home one of their top priorities.
8 Conclusions

"To innovate, you must learn to fail well. Learn from your mistakes."

- Eric Schmidt

To sum up, this thesis has achieved both objectives stated in the introductory chapter.

O1: Explore the rationales behind the emerging trend of the smart home to establish the importance of this market, and to clarify the high-level goals for the smart home. (Chapter 3)

O2: Understand the criticality of the cybersecurity requirement, various dynamics forces at play and the consequences of not meeting it in the smart home. (Chapter 4, 5, and 6)

Based on the analysis of four dynamics forces at play - 1) macro pressures to innovate, 2) growing peril of cybercrimes, 3) vulnerabilities of the smart home, and 4) the values at risk - the conclusions can be summarized as follows:

1. The smart home innovation can have significant and far-reaching impacts on society and business due to its potential role in addressing many of the urgent challenges facing our time. Therefore, the smart home should be one of the most urgent application areas of the IoT to invest in.

2. Poor cybersecurity is currently affecting nearly every type of smart home device, and is not being taken seriously by manufacturers; as a result, cybersecurity is currently a key factor that is delaying the smart home's mainstream adoption.

3. Poor cybersecurity in the smart home can potentially lead to significant financial, privacy and even physical damage, and raise serious questions of liability for device makers with potential domino effects across the entire IoT industry.

4. Poor market reception can demotivate continued investment and innovation in the smart home space and shift companies' focus into other IoT application areas or even other industries.

5. The smart home should be considered as one system, not as separate products; cybersecurity is a system property, and therefore, should be designed in the early conceptual phase of the smart home system.
6. The entire IoT industry is one system, and what's happening in one area will not just have isolated effects, but will also impact other application areas of the IoT. Therefore, the IoT cybersecurity from the smart home to other domains should be taking seriously by all stakeholders.

7. As the smart home products become more ubiquitous and permeate every corner of life and work, all corporate leaders should rethink the boundary of cybersecurity for their firms.

8. Device manufacturers should assume that their products and associated supporting infrastructure will be attacked and they can be sued, and hence proper response procedures and counter-measures should be in place to mitigate damage.

9. For the IoT to truly live up to its huge social and economic expectations, cybersecurity needs be an urgent priority for all technology and business leaders.

In the end, it's the company that can truly win the hearts and trust of consumers that will have a sustainable business proposition, and it's the industry leaders who can solve tomorrow's problems that will profit from it well. Whoever can solve this issue will not only harness significant return on investment but also have a positive and long-lasting global impact on this generation and beyond.

8.1.1 Future Work

"Smart cyber security is no longer about just preventing a breach, but building the resiliency and the flexibility to respond to and minimize the potential negative outcomes of a breach."

- Joshua Douglas, CTO, Raytheon

Despite the best effort, this thesis maybe opens more questions than it first set out to investigate. Below is a list of suggested follow-up studies:

1. This thesis presents a qualitative analysis. But it would be interesting to gain a clear quantitative understanding, from various stakeholders' perspectives, of the security risks and the potential future risks, the estimated economic costs of various severity levels of breaches when they occur along with the estimated costs to mitigate these risks and make the home more resilient.

2. It would be interesting to see improvements and extensions to the causal loop diagram. Improvements and extensions include to have it operationalized, parameterized, and simulated with data to answer some of the "what if"
questions such as what would cause the smart home industry to be on hiatus as too many failed innovations might cause the experts to stop investing.

3. Colonel Bill Young's dissertation introduced an extension to the STPA method mentioned earlier called STPA-Sec for security analysis specifically. STPA-Sec is best suited for early design stage. It would be interesting to apply STPA-sec to analyze security requirements for the smart home system.

4. A more in-depth analysis of how the cybersecurity risks of the smart home are different from or similar to the cybersecurity risks in the other IoT domains would help improve the understanding of cybersecurity challenges in various IoT categories.

5. A clear understanding of the impact of the proliferation of electronic sensors on the environment and the comprehensive lifecycle of the IoT technology would be important to make IoT truly sustainable.

6. An analysis of how various innovations of the smart home should be prioritized, separating the most urgent innovations from the bells and whistles, the must-haves from the nice-to-haves would help the industry to focus on the most urgent innovations first.

8.1.2 Final Thoughts

“The strength of a nation derives from the integrity of the home.”

- Confucius

Finally, recall Carl Fredrickson's flying house as in the popular 2009 Disney movie Up? From community apartments to large mansions, from space capsules for astronauts in interstellar stations to a rut in the deepest of the jungle, from the world's smallest house to as large as an entire country to an entire planet, there are many views that can challenge the conventional idea of the home. But none of them should change its fundamental functions to provide safety and security to its occupants, that it is the physical establishment that is most profoundly close to us all.
9 Appendix A: Threat Landscape Infographic (Symantec, 2016)

**BIG NUMBERS**

**BREACHES**
- **Total Breaches**
  - 2013: 253
  - 2014: 312
  - 2015: 305
- **Breaches With More Than 10 Million Identities Exposed**
  - 2013: 8
  - 2014: 4
  - 2015: 9
- **Average Identities Exposed per Breach**
  - 2013: 2.2M
  - 2014: 1.1M
  - 2015: 1.3M
- **Median Identities Exposed per Breach**
  - 2013: 6,777
  - 2014: 7,000
  - 2015: 4,885

**EMAIL THREATS, MALWARE AND BOTS**

- **Overall Email Spam Rate**
  - 2013: 66%
  - 2014: 60%
  - 2015: 53%
- **Email Phishing Rate (Not Spear Phishing)**
  - 2013: 1 in 392
  - 2014: 1 in 965
  - 2015: 1 in 1,846
- **Email Malware Rate (Overall)**
  - 2013: 1 in 196
  - 2014: 1 in 244
  - 2015: 1 in 220
- **Number of Bots**
  - 2013: 2.3M
  - 2014: 1.9M
  - 2015: 1.1M

- **New Malware Variants (Added in Each Year)**
  - 2014: 317M
  - 2015: 431M

- **Crypto-Ransomware Total**
  - 2014: 269K
  - 2015: 362K

- **Average Per Day**
  - 2014: 737
  - 2015: 992
Appendix B: Threat Landscape Infographic

(Symantec, 2016)
## Appendix C: Hacking Products Price List 1
(Dell SecureWorks, 2016)

### Credit Cards

<table>
<thead>
<tr>
<th>Credit Card</th>
<th>Price in 2013</th>
<th>Price in 2014</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa and MasterCard (U.S.)</td>
<td>$4</td>
<td>$4</td>
<td>$7</td>
</tr>
<tr>
<td>Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data</td>
<td>$12</td>
<td>$12</td>
<td>$15</td>
</tr>
<tr>
<td>Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data</td>
<td>$19 – $20</td>
<td>$19 – $20</td>
<td>$25</td>
</tr>
<tr>
<td>Visa Classic and MasterCard Standard (EU) with Track 1 and 2 Data</td>
<td>$28</td>
<td>$28</td>
<td>$40</td>
</tr>
<tr>
<td>Visa Classic and MasterCard Standard (U.K.) with Track 1 and Track 2 Data</td>
<td>$19 – $20</td>
<td>$19 – $20</td>
<td>$40</td>
</tr>
<tr>
<td>Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data</td>
<td>$28</td>
<td>$28</td>
<td>$50</td>
</tr>
<tr>
<td>Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Premium Visa and MasterCard (EU and U.K.) with Track 1 and 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$50 – $60</td>
<td></td>
</tr>
<tr>
<td>Premium Visa and MasterCard (Canada, Australia and New Zealand) with Track 1 and Track 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$35 for V and MC</td>
<td></td>
</tr>
<tr>
<td>Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$80 for V and MC</td>
<td></td>
</tr>
<tr>
<td>Premium American Express Card (U.S.) with Track 1 and Track 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Premium Discover Card (U.S.) with Track 1 and Track 2 Data</td>
<td>$23 (V); $35 (MC)</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>VBV (U.K., Australia, Canada, EU and Asia)</td>
<td>$17 – $25</td>
<td>$28</td>
<td>$25</td>
</tr>
</tbody>
</table>

### Hacking Email and Social Media Accounts

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)</td>
<td>$129</td>
</tr>
<tr>
<td>Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)</td>
<td>$65 – $103</td>
</tr>
<tr>
<td>Popular Ukrainian Email Accounts (Ukr.net)</td>
<td>$129</td>
</tr>
<tr>
<td>Popular U.S. Social Media Accounts</td>
<td>$129</td>
</tr>
<tr>
<td>Popular Russian Social Media Accounts (VKru and Ok.ru)</td>
<td>$194</td>
</tr>
<tr>
<td>Corporate Email Accounts</td>
<td>$500 per mailbox</td>
</tr>
<tr>
<td>IP address of Computer User</td>
<td>$90</td>
</tr>
</tbody>
</table>

### Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Price in 2013</th>
<th>Price in 2014</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Access Trojans (RATs)</td>
<td>$50 – $250</td>
<td>$20 – $50</td>
<td>$5 – $10</td>
</tr>
<tr>
<td>Crypters</td>
<td>N/A</td>
<td>$50 – $150</td>
<td>$80 – $440</td>
</tr>
<tr>
<td>Angler Exploit Kit</td>
<td></td>
<td></td>
<td>$100 – $135</td>
</tr>
</tbody>
</table>
## Appendix D: Hacking Products Price List 2
(Dell SecureWorks, 2016)

### Identities, Passports, Social Security Cards and Other Documents

<table>
<thead>
<tr>
<th>Service</th>
<th>Price in 2013</th>
<th>Price in 2014</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Fultz</td>
<td>$25</td>
<td>$30</td>
<td>$15 - $65</td>
</tr>
<tr>
<td>Fultz (Canada, U.K.)</td>
<td>$30 - $40</td>
<td>$35 - $45</td>
<td>$20 (Canada) $25 (U.K.)</td>
</tr>
<tr>
<td>U.K. Passport Scan</td>
<td></td>
<td>$25</td>
<td></td>
</tr>
<tr>
<td>Physical Counterfeit Passports (non-U.S.)</td>
<td>N/A</td>
<td>$200 - $500</td>
<td>$1,200 to $3,000 (European)</td>
</tr>
<tr>
<td>Physical Counterfeit Passports (U.S.)</td>
<td></td>
<td></td>
<td>$3,000 to $10,000</td>
</tr>
<tr>
<td>Templates for U.S. Passports</td>
<td></td>
<td></td>
<td>$100 - $300</td>
</tr>
<tr>
<td>New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill</td>
<td>$250; matching utility bill an additional $100</td>
<td>$90</td>
<td></td>
</tr>
<tr>
<td>Physical Counterfeit Social Security Cards</td>
<td>$250 - $400</td>
<td>$140 - $250</td>
<td></td>
</tr>
<tr>
<td>Scans of Counterfeit Driver's License</td>
<td></td>
<td>$14 - $20</td>
<td>$14 (U.K., CANADA)</td>
</tr>
<tr>
<td>Physical Counterfeit Driver's License (France)</td>
<td></td>
<td></td>
<td>$238</td>
</tr>
<tr>
<td>Physical Counterfeit Driver's License (U.S., U.K., Germany, Israel, International Driver's Permit)</td>
<td>$100 - $150</td>
<td>$173</td>
<td></td>
</tr>
</tbody>
</table>

### Online Accounts

<table>
<thead>
<tr>
<th>Service</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Popular U.S. Online &quot;Business&quot; Payment Account Credentials</td>
<td>Ranges from $20 - 149</td>
</tr>
<tr>
<td>Transfer Funds from Popular Online Payment Account to Buyer's Account of Choice</td>
<td>$750 cost $226</td>
</tr>
<tr>
<td></td>
<td>$1,500 cost $377</td>
</tr>
<tr>
<td></td>
<td>$1,520 cost $385</td>
</tr>
<tr>
<td></td>
<td>$2,290 cost $573</td>
</tr>
<tr>
<td></td>
<td>$2,999 cost $750</td>
</tr>
<tr>
<td></td>
<td>$3,799 cost $950</td>
</tr>
<tr>
<td>Popular U.S. Online Payment Account Credentials</td>
<td>$330 cost $80</td>
</tr>
<tr>
<td></td>
<td>$400 cost $160</td>
</tr>
<tr>
<td></td>
<td>$500 cost $240</td>
</tr>
<tr>
<td></td>
<td>$600 cost $320</td>
</tr>
<tr>
<td></td>
<td>$950 cost $600</td>
</tr>
</tbody>
</table>
### Appendix E: Hacking Products Price List 3 (Dell SecureWorks, 2016)

#### Bank Accounts; Airline and Hotel Points

<table>
<thead>
<tr>
<th>Bank Account Credentials</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank accounts — ANZ (Australia)</td>
<td>Price based on account balance</td>
</tr>
<tr>
<td>Bank accounts — ANZ (Australia)</td>
<td>$18,000 cost $4,750</td>
</tr>
<tr>
<td>Bank accounts — ANZ (Australia)</td>
<td>$22,000 cost $2,250</td>
</tr>
<tr>
<td>Bank accounts — ANZ (Australia)</td>
<td>$62,567 cost $3,800</td>
</tr>
<tr>
<td>Bank accounts with no balance listed — Turkey, Sweden, Norway, Romania, Bulgaria, Croatia.</td>
<td>$400 (flat fee)</td>
</tr>
<tr>
<td>Bank accounts — (U.K.)</td>
<td>$27,003 cost $2,000</td>
</tr>
<tr>
<td>Bank account — (U.S.)</td>
<td>$1,000 cost $40</td>
</tr>
<tr>
<td>Bank account — (U.S.)</td>
<td>$2,000 cost $80</td>
</tr>
<tr>
<td>Bank account — (U.S.)</td>
<td>$4,000 cost $150</td>
</tr>
<tr>
<td>Bank account — (U.S.)</td>
<td>$7,000 cost $300</td>
</tr>
<tr>
<td>Bank account — (US.)</td>
<td>$15,000 cost $500</td>
</tr>
</tbody>
</table>

#### High Quality Bank Accounts with Verified, Large Balances of $70,000 - $150,000

<table>
<thead>
<tr>
<th>Price based on points in account</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,500,000 points cost $450</td>
</tr>
<tr>
<td>300,000 cost $90</td>
</tr>
<tr>
<td>200,000 cost $60</td>
</tr>
</tbody>
</table>

#### Large U.S. Airline Points Accounts — varies based on amount

<table>
<thead>
<tr>
<th>Price based on points in account</th>
</tr>
</thead>
<tbody>
<tr>
<td>500,000 cost $150</td>
</tr>
<tr>
<td>450,000 cost $90</td>
</tr>
<tr>
<td>250,000 cost $50</td>
</tr>
</tbody>
</table>

#### Large Middle East Airline Points Accounts — varies based on amount

<table>
<thead>
<tr>
<th>Price based on points in account</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000 points cost $200</td>
</tr>
<tr>
<td>400,000 cost $80</td>
</tr>
<tr>
<td>300,000 cost $60</td>
</tr>
<tr>
<td>200,000 cost $40</td>
</tr>
<tr>
<td>100,000 cost $20</td>
</tr>
<tr>
<td>50,000 cost $10</td>
</tr>
</tbody>
</table>

#### Large International Hotel Chain Points Account

<table>
<thead>
<tr>
<th>Price based on points in account</th>
</tr>
</thead>
<tbody>
<tr>
<td>$20 to $40 for multiple tutorials</td>
</tr>
</tbody>
</table>

### Hacking Services

<table>
<thead>
<tr>
<th>Hacking Tutorials</th>
<th>Price in 2013</th>
<th>Price in 2014</th>
<th>Recent Prices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking Tutorials</td>
<td>N/A</td>
<td>$1 each to $30 for 10 (depending on the tutorial)</td>
<td>$20 to $40 for multiple tutorials</td>
</tr>
<tr>
<td>Hacking Website (stealing data)</td>
<td>$100 - $300</td>
<td>$100 - $200</td>
<td>$350</td>
</tr>
<tr>
<td>DDoS Attacks</td>
<td>Per Hour: $3 - $5</td>
<td>Per Hour: $3 - $5</td>
<td>Per hour: $5 - $10</td>
</tr>
<tr>
<td></td>
<td>Per Day: $90 - $100</td>
<td>Per Day: $60 - $90</td>
<td>Per Day: $30-$55</td>
</tr>
<tr>
<td></td>
<td>Per Week: $400 - $600</td>
<td>Per Week: $350 - $600</td>
<td>Per Week: $200 - $555</td>
</tr>
<tr>
<td>Doxing</td>
<td>$25-$100</td>
<td>$25-$100</td>
<td>$19.99</td>
</tr>
</tbody>
</table>
Appendix F: 2016 IoT Landscape (Turck, 2016)


Goodin, D. (2015). Adobe Flash exploit that was leaked by Hacking Team goes wild; patch now! Retrieved April 17, 2016, from http://arstechnica.com/security/2015/07/adobe-flash-exploit-that-was-leaked-by-hacking-team-goes-wild-patch-now/


