Suggested Citation: https://dx.doi.org/10.2139/ssrn.3022111

The Internet of Things (IoT) Promises New Benefits — and Risks:

A Systematic Analysis of Adoption Dynamics of IoT Products

Mohammad S. Jalali, Jessica P. Kaiser, Michael Siegel, and Stuart Madnick

Abstract—The Internet of Things (IoT) aims to translate our physical world into digital signals, ripe for the improvements promised by faster communication and better analytics. One of the greatest obstacles to broad adoption of IoT is the introduction of cyber risk – real and perceived – to buyers. We aimed to understand the mechanisms by which cybersecurity influences IoT adoption, using system dynamics to develop these mechanisms into a qualitative causal loop diagram. We conducted a case study of commercial building applications of a connected lighting product. Our analyses revealed that potential customers decide to adopt IoT technologies based on their perception of risk-reward ratio. Internet of Things producers need to improve that ratio by developing clear, measureable product benefits in tandem with customer support models that address cyber risk. They should create cybersecurity capabilities at the beginning of their market growth, from identifying and addressing cyber risk in product design to detailed cyber-incident response plans with clear action items and owners. Furthermore, IoT start-ups are particularly vulnerable to the tradeoffs between immediate revenue through accelerated market adoption and risked future revenue from security vulnerabilities. The common rush to build IoT products before securing them will make them potentially vulnerable to cyber-incidents.

Index Terms— Business-case analysis, Cyber-physical systems, Internet of Things, Modeling

1 Introduction

THIS research aims to better understand the mechanisms by which cybersecurity will influence Internet of Things (IoT) technology adoption. Security challenges include the unintended consequences of focusing on innovation and marketing to power growth of a product, while leaving it vulnerable to hacking, the tension between prioritizing product usability and product security. Another important question is what standards will emerge in the IoT marketplace. How will they prove themselves to the market as secure? Will the market by dominated by a few key players, or will the market remain highly fragmented, with high firm entry and exit?

Despite the growing literature of cybersecurity, the direct mechanics by which cybersecurity might impact IoT adoption have not been studied. Given the IoT's unique vulnerabilities and relative infancy in the marketplace, it is unclear what the impact of a cyber-incident might be on IoT product adoption. Will IoT products experience the rapid "hockey stick" growth exhibited by tech companies like Facebook (the green line in Figure 1)? Or, might publicized cyber-incidents so hamper the growth of an IoT product that it never gets off the ground (the "start-and-fizzle" red dotted line in Figure 1)? Or, is the reality somewhere between these two extremes—the "still successful" and "partially successful" red dotted lines in Figure 1? Furthermore, will growth occur for the market as a whole, or will a few dominant players emerge? If the latter, will those players be mature companies or start-ups?

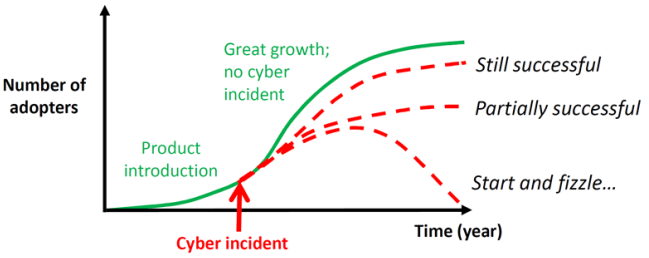

Fig. 1. A range of product adoption curves in response to a cyber-incident. A better understanding of how product adoption may be affected by a breach can guide managers making security investment decisions early in a product's development.

An example of a cyber-incident's effect on product sales was the "My Friend Cayla" doll - the doll was the subject of a "trash it" recommendation from the German telecommunication regulator after it was discovered that a feature of the doll—voice transmission to a U.S. based voice recognition company—was vulnerable to independent and possibly malicious hackers, as reported in the Washington Post [1].

• *M.S. Jalali, J.P. Kaiser, M. Siegel, and S. Madnick are with Cybersecurity at MIT Sloan School of Management, Cambridge, MA 02138. E-mail: jalali@mit.edu, jpkaiser@mit.edu, msiegel@mit.edu, and smadnick@mit.edu.*

We perform a case study of product development for commercial building applications of a connected lighting product at a large electronics company, using a system dynamics approach to develop these mechanisms into a qualitative causal loop diagram. This approach generates a framework that IT executives at supplier companies[1] can use in strategic decision-making to better understand what consequences—both intended and unintended—may arise from the choices they make during IoT product development. Without this systematic perspective, supplier decision makers might focus on a component of the system (e.g., innovation) and optimize it locally to achieve suitable outcomes and grow in the market; however, when feedback mechanisms from other components of the system are activated (e.g., cybersecurity mechanisms), the initially successful strategies may not only become ineffective but also exacerbate their situation in the marketplace. Therefore, it is essential to take a systematic approach, looking at the big picture of the problem and analyzing the components of the systems and their interconnections.

This article proceeds in two sections. In the first, we provide an overview of the concepts explored in our case study and model: we begin with an overview of the Internet of Things. We then describe the basics of diffusion models, and describe in greater detail a concept that our research showed to be a great influence on IoT technology purchase decisions – the risk-reward ratio. We then describe current cybersecurity standards for technology purchase decisions. In the second section, we enter the case study, describing the IoT product market studied, the model derived from our research, and its implications. Finally, we close with a four cybersecurity-related guidelines that managers can use to influence market adoption of IoT products.

2 Overview of Concepts

2.1 Introduction to Internet of Things (IoT)

"[Connected systems are] about giving you data to make your space more optimized."

"Getting more data into the system… it'll become more interesting to hack the system."

"Connected systems are too big of an opportunity to miss because we have some jerks who are hacking into things." – Potential IoT Adopters

The Internet of Things (IoT) aims to translate our physical world into digital signals, ripe for the improvements promised by faster communication and better analytics. While there is no universally agreed upon definition of the IoT, the Internet Society [2] shows that most definitions converge to describe systems that collect data from the physical world on devices used to process information, in addition to providing a good summary that explores the benefits and challenges of the IoT. Often, the digital processes are intended to produce kinetic effects, and rely heavily on networking with other external devices. These innovations are made possible by the declines in the cost of computing and simultaneous improvements in sensor performance and range. Examples of settings where the IoT might be deployed vary from the intimate, like personal health data, to the massive, such as a connected system of street lights, parking meters, transit, and autonomous vehicles that might be used to collect useful municipality data and optimize delivery of city services to citizens. The potential value generated by IoT is estimated to be at least $3.9 trillion and up to $11.1 trillion by 2025, with the higher estimate representing 11% of projected global GDP in the same year, as shown by Manvika et al. [3].

One of the greatest obstacles to broad market adoption of IoT technology is the introduction of cyber risk – real and perceived – to buyers. The Open Web Application Security Project [4] described Internet of Things technologies as having three unique weaknesses with regards to cybersecurity: (1) high numbers of endpoints, (2) inconsistent protocols, and (3) physical safety concerns. Verizon [5] estimated in a 2015 report that the number of IoT endpoints will grow from 9.7 billion in 2014 to 30 billion in 2020. As of today, the mechanisms to manage consistent endpoint security over a system so vast do not exist. Furthermore, the diversity of standards across the IoT defrays the responsibility of any single actor in the technology chain for security. As of writing, there are two commercially available "certification programs" for IoT Security from Underwriter Laboratories and ICSA Labs, an independent division of Verizon. Both were launched in 2016, and have met some skepticism, as noted in an article in The Register [6]. Lastly, because the IoT represents a linked set of physical devices, it presents the opportunity for malicious actors to move their criminal activities—previously confined to cyber space—into the physical world.

These characteristics of IoT cybersecurity are not merely pedantic, they are actively being exploited. This is perhaps best exemplified by a large scale, distributed denial-of-service (DDoS) attack that took place in 2016. In the time leading up to the attack, AT&T [7] tracked a 400% increase in scans of IoT ports and protocols. The attackers took advantage of mostly unaltered default passwords across a huge number of IoT devices to hobble the critical infrastructure of the internet. Attacks like this have also been documented in private organizations, where the quantity of nodes are used to overwhelm a network with traffic, such as the one reported by Cyberscoop [8] against a university.

Lastly, both individual and organizational adopters of IoT have concerns about its security and privacy implications. For example, the 2015 Icontrol State of the Smart Home study [9] found that over 40% of Americans were

[1] Throughout the article, we refer to customer organizations as "adopters", and organizations that produce IoT products as "suppliers". While the intended audience for the paper is supplier organizations, we discuss the mindset and behaviors of adopting organizations, and use this nomenclature to make it clearer to whom we are referring.

very concerned about the possibility of their information being stolen from their smart home. Furthermore, it has been noted by potential regulators in the Federal Trade Commission [10] that such concerns may prevent these technologies from reaching their full potential, although it is not clear how it alters the consumer's purchase decision. Security concerns are heightened for organizational adopters in industries with increased exposure to technology, like banking, defense, and healthcare.

2.2 Basics of Diffusion Model of Technology

One of the most influential adoption models in technology products is the 'Bass diffusion model'. Our framework expands on this model by including the influence of additional market factors related to cybersecurity; however, understanding our new model requires a review of the original Bass diffusion model. Diffusion describes the process by which an innovation spreads and explains the typical "S-curve" seen in product adoption: The user base is small to start, then increases as adoption increases, and eventually approaches the limit of the potential market. The S-curve has been observed in the diffusion of many diverse innovations, such as electricity, the washing machine, and most recently, social media networks like Facebook. This is represented by the green line in Figure 1.

Vernandikis [11] premises the underlying Bass diffusion model on an understanding of the diffusion process as an epidemic. The innovation spreads by information exchange, and time lags between potential users and installed users explain the observed S-curve. In addition to potential users and installed users, some entities (firms or individuals) learn about the innovation but do not adopt it. This suggests that there is an adoption process, which is decomposed into phases in the literature for ease of comprehension and analysis. These phases are: (1) awareness, (2) consideration, (3) opinion formation, and (4) implementation.

A crucial variable in diffusion models is the speed of diffusion, which is affected by several factors. A critical factor affecting the speed of diffusion is what relative advantage the innovation provides. The relative advantage is the amount by which the innovation improves upon previous circumstances. The size of the population of potential adopters is another such factor, as a larger population creates more opportunities for information sharing about the innovation. The information channels and the supplier's ability to affect these channels are also powerful forces affecting information transmission.

A feature of the Bass diffusion model is that it leads to "winner take most" scenarios, since all it takes is an information exchange to catalyze the innovation adoption process. Systems scientists have articulated "the tipping point" as the point at which adoption begins to grow so quickly that one supplier can become market dominant, simply by riding a wave of rapid adoption. As such, standards play an important role in innovation diffusion. If a product can demonstrate that it is compliant, the friction and delays that would otherwise present themselves during the "opinion formation" stage are reduced. Many supplier companies try to become the standard in their industry, and reach the tipping point.

Krishnan, Bass, and Kumar [12] show that additional late entrants into an innovation marketplace can sometimes hasten the speed of diffusion, although the evidence is mixed with regards to how it impacts the incumbent's market share. For start-ups, this is a powerful incentive to enter the marketplace, as they can capture sales growth by accelerating the speed of diffusion for the overall technology. For both mature companies and start-ups, this presents a conundrum as to developing standards. On the one hand, it might be better to achieve immediate revenue by adopting another company's standard, and reducing decision friction for customers. On the other, a firm trying to create its own standards might be able to prevent other firms from entering the marketplace and reducing their market share.

2.3 The Risk-Reward Ratio: IoT's Relative Advantage to the Status Quo

"The companies that I know that are adopting CLS all have the view that 'this is innovative and that we are first adopters'."

"[Cybersecurity] is more a concern for late-majority adopters." – Product Managers

Within the context of IoT technologies, a relative advantage is to what degree connecting an object to a physical network improves the adopter's operations. Often it is the data that IoT devices produce that creates the relative advantage. In our research, we identify this as the "risk-reward ratio", noting that as the granularity and utility of data produced by an IoT product increases, security and privacy risks increase as well.

With many firms eager to capitalize on data, a cursory glance may suggest that an IoT product's relative advantage would be enormous: some data must be better than no data. However, not every IoT product sees as rapid an adoption process as might be expected, e.g. while many individuals are installing connected thermostats, few are connecting their microwave, and connecting stove knobs is unheard of, despite the benefit that cooking data could bring.[2] As we will explore, in the case of commercial building operators, businesses have been quicker to adopt connected HVAC systems than they have been to adopt connected lighting, despite cost savings benefits across both products. It must be the case then, that there are drawbacks to an IoT product, decreasing its relative advantage.

These are just two examples of IoT products in building technologies. Other examples might be in plumbing or in physical security. "Connecting" these infrastructures

[2] These are not idle examples; both connected microwaves and connected stove knobs exist. See the products Maid and Klove Knob, respectively.

can provide multiple benefits, most frequently central control and visibility that allow building managers to manage their use and maintenance more efficiently. More benefits for connected lighting systems, in particular, will be explored over the course of this article.

2.4 Cybersecurity Standards in Technology Adoption Decisions

It is valuable to review how practitioners assess security risk in technology purchase decisions; however, because cybersecurity as a discipline is in rapid evolution, practitioners have not yet arrived at consistent, universal standards for evaluating cybersecurity risk. A good sense of the variety and quantity of proposed frameworks can be obtained is discussed by Bayuk et al. [13], in a publication released prior to the development of the NIST framework discussed here. The leading framework that has emerged is the NIST Cybersecurity Framework [14], born out of a 2013 Executive Order and now in Draft Version 1.1. The Framework provides a high level, industry- and technology-neutral application of the principles of risk management to technology infrastructure, as discussed by Scofield [15]. It provides direction on steps organizations should take to improve cybersecurity iteratively. These seven steps are the ones that an adopting organization would use to adopt a new technology, and they roughly align with the adoption process explored above in the Bass diffusion model. At a high level, these steps are:

1. Prioritize and scope
2. Identify assets and risk appetite
3. Evaluate baseline performance
4. Conduct risk assessment
5. Draft target goals
6. Evaluate gap between target and actual
7. Decide, and if appropriate, adopt.

One critique by adopters of the IoT is that no standards currently define the market. Suppliers have a mixed perspective: on the one hand, the lack of standards is a possible strategic advantage, particularly for start-ups, where the lack of standards makes it easier to enter the market. On the other, the lack of standards make it difficult to articulate to adopters how to manage cyber risk. The NIST framework is technology-neutral precisely because no standards yet exist, and the government has been ineffective at creating and enforcing standards for the technology industry, leaving it instead to private players. Taken together, these facts suggest that we are early in the adoption process of the IoT as a whole, and before "winner take most" effects take hold in the marketplace, presenting a potentially lucrative market opportunity for IoT suppliers, start-ups and incumbents alike.

3 Adoption of Connected Lighting Systems

3.1 Case Study Approach to Effects of Cybersecurity on Adoption of Connected Lighting Systems

"Right now, [customers] can't see the reward [of IoT]. We can't install products. We can't show the benefits because we don't meet their cybersecurity requirements." – Sales Representative

While research exists on the topics of cybersecurity, the IoT, and technology adoption individually, there is a dearth of research that articulates how each contributes to overall market adoption. In this article, we aim to approach cybersecurity and IoT adoption from a systems science perspective. We interviewed practitioners from various functions, including security, product, marketing, and sales, of a large electronics company that produces an IoT lighting product, as well as their potential adopters and experts in the industry. From these interviews, we describe the benefits and risks associated with the IoT lighting product, and a connected HVAC product that is closely associated with lighting. Based on their articulation and comparison of the risk-reward ratios for both products, we then use their responses to adjust the typical Bass diffusion model to include cybersecurity related variables. Then, we use this model to articulate implications that reflect what impact cyber-incidents might have on an IoT product market. Finally, we use these implications to outline four cybersecurity related guidelines for managers to encourage market adoption of IoT products.

This adjusted Bass diffusion model also presents some interesting questions for future research. For example, would it be possible to quantify how attractive to criminals the market is? At what size should companies aim to be interoperable? At what size should they commit to a single platform? How might a supplier firm quantify the impact of cybersecurity on price or utility? Future work would aim to quantify the variables presented in the adjusted model in order to generate answers to these questions.

3.2 Connected Lighting Systems: Product Benefits

"People are clear on the rhetoric of IoT, but not what value it delivers." - Manager for Lighting Products

There are three reasons why connected lighting systems (CLS) are one of a few building infrastructures to be singled out for a transition to the IoT: 1) They are a point of frequent interaction for building occupants; 2) There is a high number of nodes, and light bulbs are good candidates for granular data collection; and 3) There is an opportunity for personalization, as lighting is a highly individual preference. Connecting lighting systems to a network can provide both local and central control, making it easier to provide personalization and energy savings simultaneously.

Lighting systems have already benefitted from innovations that have recouped significant cost savings, without transitioning them to an IoT product. First, occupancy sensors turn lights off and on only when they are needed, without end user intervention. Second, LED light bulbs require little maintenance.

In describing the benefits of CLS, interviewees used the "$3 - $30 - $300 rule" to describe the value opportunity

of CLS.[3] Connecting lighting alone represents only a $3 per square foot per year energy efficiency cost savings opportunity, but space optimization represent $30 and employee productivity an additional $300 cost per square foot per year savings opportunities. This rule derives from ex-post facto analysis and has not been verified empirically.

Connected light bulbs can detect that a conference room is used only 20% of the time, but that desks outside the conference room are used 100% of the time. This could be a signal that the space is under-occupied, and that the conference room space could be used more efficiently. Or, consider an office building with an "open desk" policy, in which employees are not assigned to desks and can use any open space. Using motion sensors on light bulbs to detect which desks are occupied, IT systems can direct employees to an available desk when they enter the building. Practitioners believe occupancy data and space-saving systems like these represented a $30 per square foot per year cost-saving opportunity.

The "holy grail" of CLS for commercial applications is in collecting data about productivity occurring under the light bulbs. Practitioners point to articles like Baer [16] showing that lighting has a strong physiological and psychological effect on workers. Adjusting hues and saturation for a personalized environment that complement an employee's work style could generate additional productivity for a firm. Done correctly, interviewees believe this represents an enormous cost savings opportunity of $300 per square foot per year. For an average U.S. office building, these three categories represent a total cost savings of $5.2M—see Table 1.

For home rather than business adopters, the "$3-$30-$300 rule" is believed to apply directionally, but it is unlikely that adopters without the resources of a larger organization would attempt to quantify the benefits to justify their purchase. Instead, the product's relative advantage depends on how important the ability to customize lighting hues and saturation in a home environment is to the customer. Given the lack of case studies or empirical data supporting the rule, the underlying theory has yet to be proven, making the relative advantage of CLS confusing to both home and business adopters.

The confusion around the benefits of CLS stands in contrast to another building system that has been connected to the IoT: connected HVAC systems. Compared to HVAC systems, which represent 44% of energy costs in commercial buildings, lighting systems represent about only 10% of a building's energy costs [18]. Since HVAC systems contribute such a large portion of a building's energy bill, and components like chillers are more expensive to maintain proactively, connecting HVAC systems to the IoT presents immediate and easily quantifiable benefits to the adopter. Interviewees feel the ease of measurement of connected HVAC rewards means that the relative advantage is more apparent to adopters than the relative advantage of CLS. However, they felt that CLS offered potentially higher rewards that were simply more difficult to quantify.

TABLE 1
COST SAVINGS BY CATEGORY UNDER THE $3-$30-$300 RULE

Average US office building	Average square foot	15.8k
Potential savings	Energy efficiency	$47.2k
	Space optimization	$472k
	Productivity	$4.72M
	Total	**$5.2M**

Average building size is derived from the Commercial Buildings Energy Consumption Survey [17].

TABLE 2
FEATURE-EXPLOIT ANALYSIS OF CONNECTED BUILDING INFRASTRUCTURE (E.G. CLS AND HVAC)

Feature	Value	Exploit	Exploit Example
Personalization (e.g., color or temperature control)	• Greater occupant satisfaction and productivity	• Create annoyance, harassment, or physical discomfort[1] • Overload output for physical damage	• Possible for a malicious attacker to remotely access light bulbs and switch on/off (2013)
Wireless Control System	• Insight into energy, occupant utilization, and component use • Integration to improve efficiency and occupant satisfaction	• Access core IT for espionage or use in illegal activities • Methods include packet sniffing, replay, trashcan, social engineering, and others	• Hackers demonstrated first ransomware for IoT thermostats (2016)
Central and local control	• Achieve balance between energy use and occupant comfort • Greater ease of use	• Nodes create potential for DDoS attacks • Opportunity to sabotage or interfere with operations through ransomware	• IoT devices turned against university IT network in DDoS attack against itself (2017) •
Occupancy Sensor	• Greater ease of use • Space optimization • Coordinated responses • Energy efficiency	• Passive surveillance • Maximize damage during kinetic attacks • Minimize risk of being caught (e.g., burglary)	• Occupancy tracking possible through WiFi probe requests over network (2016)
Power over Ethernet	• Lower install costs • Energy reporting	• Potentially easier to disrupt • Limited security literature	• Theoretical, but no proof of concept hacks in literature

Of the above features and their associated exploits, only Power over Ethernet is unique to CLS.

3.3 Potential Cyber Risks of CLS

> *"It's so complicated that to minimize the risk, we just don't network the lighting system… it's slowed us and the market." – Director of Infrastructure Operations, responsible for over 150 networked buildings*

In describing the features of CLS most often considered prior to adoption, an important, yet confusing, aspect is the "cybersecurity" component of CLS. Interestingly, only one feature of CLS presents a cyber risk that is unique to lighting, yet interviewees are more concerned about the cyber risk exposure of CLS than about the cyber risk exposure of HVAC (See Table 2 for a list of features and their exploits across CLS). Four reasons are introduced to explain this discrepancy:

1. CLS has orders of magnitude more nodes than HVAC (e.g., multiple light bulbs in a room versus one control panel on a floor), making it more difficult to manage endpoint security;
2. The cost of a single point of failure or overload for CLS is much lower than for other building systems (e.g., less than one hundred dollars for a light bulb, versus thousands of dollars

[3] Though nearly all of the interviewees mentioned this rule, we could not locate an external source that validated the existence of this rule beyond our case study company.

for a chiller);

3. Potential adopters did not yet have the internal analytic capabilities, including sufficient data security and privacy protection, to leverage the space optimization and productivity benefits of CLS; and
4. The product and its associated service do not meet the cybersecurity standards of the adopting organization.

In connected building infrastructures, it is rare to store data of an intimately personal nature on an IoT device. However, when the IoT device processes PII or medical data, the risks for physical harm beyond discomfort increase.

4. The "Iceberg" Model

4.1 Presentation of the "Iceberg" Model

> *"We need to make it simple for them to use, so that they can put security in place. Otherwise there would be no security at all." – Security Manager*

Most supplier companies that produce new technologies, regardless of their size, create innovations that they believe present a possible solution to a customer pain point. They aim to test whether early versions of the product are attractive to customers, and if they are, use market growth to drive improvement of the product. This cycle is represented by the blue lines in Figure 2, the 'tip of the iceberg'.

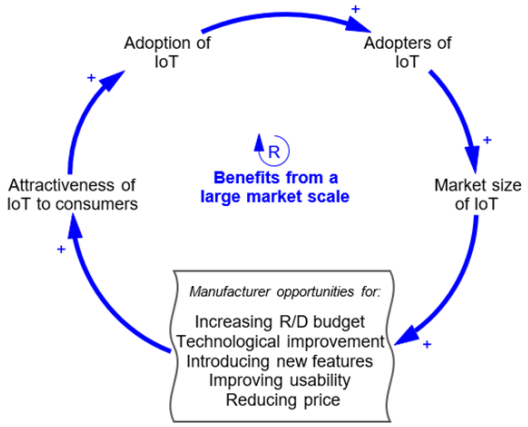

Fig. 2. The visible "tip of the iceberg". This reinforcing feedback loop describes how market adoption benefits product development.

If a consumer finds the product attractive, then the IoT product's adoption will increase when he or she adopts it—the positive sign on the arrow represents that the two variables change with the same polarity: An increase in the attractiveness causes an increase in the adoption, or a decrease causes a decrease. As "adoption of IoT" increases, so does "adopters of IoT", gradually increasing the size of the market for the product and producing more revenue for the company.[4] En masse, enough revenue is produced that the supplier company can then make resource allocation decisions to increase R&D, improve the technology and its features, make it easier to use, or reduce the price to bring in more customers. All of these, in turn, make the product even more attractive (completing the loop in Figure 2), bringing in even more customers. If the supplier company can activate this reinforcing cycle, then they can reach the "tipping point" and generate the steep growth of the S-curve explored earlier in this article.

As the model's name suggests, there are additional mechanisms operating below the surface. Reluctance to adopt CLS was attributed largely to drawbacks that were directly and indirectly related to cyber risk exposure. This suggests that there are other factors beyond "success begets success" influencing the information gathering and opinion formation phases of the adoption cycle. Several internal experts and potential adopters of the product in our case study mentioned cyber-incidents and the cyber criminal market in discussing the risks of the product. This is suggestive of the cycle presented in Figure 3 in which cybersecurity elements act as a balancing force to the other adoption mechanisms in both the adopter and the supplier's direct control.

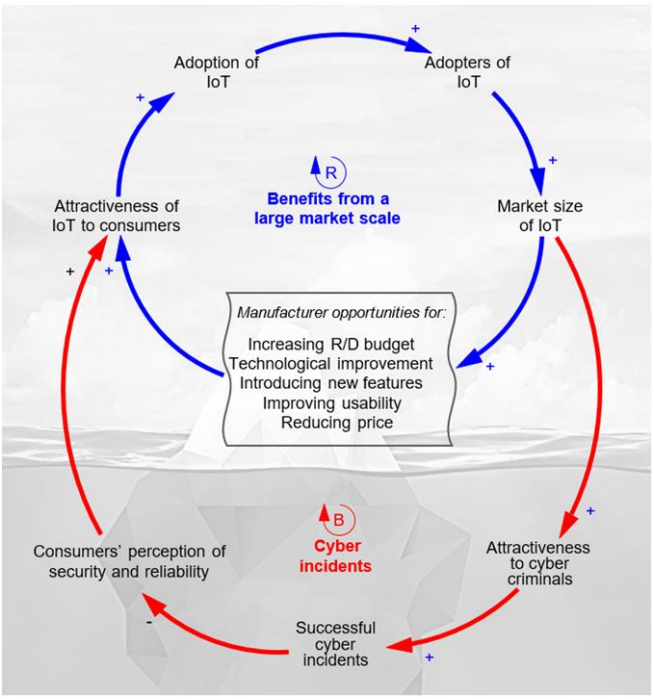

Fig. 3. The "iceberg" model. The balancing loop works against the reinforcing loop to limit the potential growth of the product, but is not necessarily visible to product managers unless they experience a cyber incident.

In the model presented in Figure 3, cyber risk exposure is part of a customer's perception of security and reliability, and affects the relative advantage of the IoT product.

As its adoption increases, a product becomes more attractive to hackers and it is likely that some attacks will succeed. If attacks become known to customers, the perceived security and reliability of the product will diminish

[4] We distinguish between adoption and adopters of IoT, as adoption is a rate, whereas adopters are a number.

(see the balancing loop 'cyber-incidents' in Figure 3). While a supplier company is focused on introducing additional features, potential adopters may decide that the cyber risk exposure is too great to justify the benefits of the product or any number of novel features. Thus, the activity of the cyber criminal market, in red in Figure 3, becomes an unintended, countervailing force on the activities of the manufacturer, in blue.

4.2 Implications of the "Iceberg" Model

"The incremental gain relative to the risk that you have for a connected lighting system is less prominent than HVAC... You don't need a fully connected lighting system to make energy savings use cases work." – Potential CLS Adopter

"You can spend 15-20 years building up your brand, and a cyber attack can crush it in 2 or 3 minutes."

The counterforce mechanism of cyber criminal activity on market adoption (the red loop in Figure 3) may slow adoption of IoT products, explaining why IoT has not yet reached a 'tipping point'. It may also explain why the potential adopters to whom we spoke are reluctant to adopt CLS products as compared to HVAC products, despite well-publicized HVAC cyber exploits. The cost saving opportunity of CLS products in the "space optimization" and "productivity" categories is not yet fully realized due to the fact that most adopters are still building internal analytic capabilities, so only the smaller benefits of energy efficiency are immediately recovered by adopters. A cyber-incident targeting CLS this early in its adoption cycle might have a great impact on the market.

A place where the red and blue loops in Figure 3 come into tension is in improving the product's usability, since security features are often seen by customers as inconveniences. One example that many customers experience is the difficulty of remembering long, complex passwords. A supplier company could choose to activate the blue loop by requiring no password at all, making the product more usable, but vulnerable to hackers. An increase in cyber-incidents would soon result in customers no longer perceiving the product as secure or reliable. In practice, few supplier firms would remove password requirements in response to customer feedback, but the tension between usability and security was brought up by interviewees. The product must be simple enough to attract customers, yet secure enough to reduce the likelihood of successful cyber-incidents.

4.3 Cybersecurity Capability Development

"From what I know of this, it seems that the likelihood of getting an attack is like 100%!" – Potential IoT Adopter

"Security should *be a given." – Product Manager [emphasis added]*

"I certainly feel like I need more support. The minute customers ask about cybersecurity and firewalls, I can't speak to it on the level I'd like to." – Sales Manager

Fighting back against cyber criminals is a decision that management from supplier companies must make in the initial stages of market growth (shown by the green decision arrows in Figure 4). Consider an example of two hypothetical IoT supplier start-ups: one chooses to invest in cybersecurity capabilities as they begin to grow, while the other does not. Typically, cybersecurity capabilities are the 5 recommendations of the NIST Framework: Identify, Prevent, Detect, Respond, and Recover. As their market size approaches a scale that makes them attractive to cyber criminals, the organization that invested in its capabilities is less likely to be on the receiving end of a successful cyber attack and will ultimately be more successful than the competitor that did not invest in cybersecurity capabilities, thanks to its reputation of security and reliability. While not explored in this framework, there are likely also market adoption mechanisms at play in the cyber criminal market. The competitor who did not invest in cybersecurity capabilities may gain a reputation for being an easy mark, making them an even greater target for cyber criminal activity.

It is important for a supplier firm to invest in cybersecurity as a proactive, preventative measure. In a large, resource-rich organization, this might mean prioritizing security during resource allocation, and working to become the standard for security in the IoT industry, reaching closer to the tipping point. In a resource-scarce organization, like an IoT start-up struggling for cash, people, and time, there is a trade-off between focusing on reaching the tipping point to achieve stable revenues that can be invested in security, and focusing on security right away at the expense of attracting early customers. Jalali, Seigel, and Madnick [19] show that even experienced managers have difficulties overcoming decision making biases when building cybersecurity capabilities. Furthermore, it is not clear whether perception and reality are well aligned when it comes to security. In MIT's "House of Security" study [20], it was shown that executives show a significant gap in assessing their organization's vulnerability, relative to lower- and mid-level employees.

Despite the criticisms, one place to start in assessing current and developing target cybersecurity capabilities is the NIST Framework. The Framework positions five concurrent functions – Identify, Protect, Detect, Respond, and Recover – as critical to having comprehensive cybersecurity capabilities.

The "iceberg model" shows there are no easy answers. But, if a supplier organization of any size hits the tipping point too quickly without the necessary cybersecurity capabilities, they risk losing market share later during a

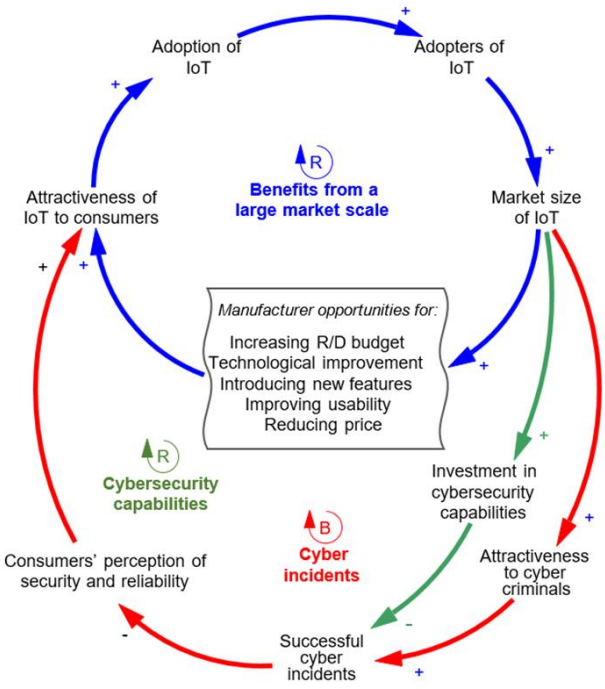

Fig. 4. Fighting back. To limit the effects of the cyber incidents balancing loop, product developers must also invest in developing cybersecurity capabilities in order to get the full benefits of robust market adoption.

cyber-incident. In the next section, we discuss several cybersecurity recommendations for supplier organizations to make IoT product adoption more resilient to cyber-incident.

5 Cybersecurity Focused Guidelines for Robust and Resilient Market Adoption

Managers of IoT products should consider these four guidelines, informed by our model, to grow market size and keep their market resilient to cyber-incidents.

1. **Capture data at the granularity that shows measureable benefits for customers – and no lower:** The benefits of many IoT technologies cannot be fully realized without granular data capture and processing. Too granular, however, and two things happen: 1) cyber risk exposure increases considerably and 2) product benefits become more difficult to understand and capture. In both cases, market adoption slows. When expanding into new market features where more granular data is required, partner with firms with strong analytics capabilities and data protection practices for case studies that show measureable benefits.
2. **Measure and monitor your product's risk-reward ratio:** The risk-reward ratio measures the benefits and risks of adopting a new technology, and can help you understand the potential impact of a cyber-incident on market adoption. It can also guide investment decisions as you develop the product or its new features.
3. **Invest in cybersecurity capabilities from product design to sale to on-going support:** Cybersecurity expertise is required not only to build security into your product and processes, but to explain it to your customers. As cybersecurity becomes a top-of-mind concern for all customers, it will become more important to have experts with every customer touchpoint who can address concerns, prevent and detect threats, and respond to incidents. This includes a detailed incident response plan with clear actions and owners. Make sure ownership transfer is a part of succession planning, and conduct regular reviews of the response plan to ensure that it remains up-to-date.
4. **Take responsibility for security along your technology supply chain up to the last mile:** If you choose to develop on a platform, choose a platform with a reputation for strong security. If you develop your own platform, work with 3rd parties to certify its safety. If creating hardware, buy from manufacturers with certifications and reputations to uphold. Only allow customers to customize the final layer of the product to ensure that built-in protections cannot be overridden.

Acknowledgment

We would like to thank Kristin Dahl, Jerrold Grochow, Allen Moulton, Natasha Nelson, and Kris Winkler for providing constructive feedback and comments on earlier versions of this article. We would also like to thank all the individuals who agreed to be interviewed for our research. Their time and expertise in building and validating this model is appreciated. Financial support for this study was provided by MIT (IC)3—the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

References

[1] A. Erickson, "This pretty blond doll could be spying on your family," *Washington Post*, Feb 23, 2017.

[2] Internet Society. "The Internet of Things (IoT): An Overview," https://www.internetsociety.org/resources/doc/2015/iot-overview, 2015.

[3] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world, June 2015.

[4] Open Web Application Security Project. "Internet of Things (IoT) Project," https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project, 2017.

[5] Verizon Report, "State of the Internet of Things Market Report 2016," 4 Sept, https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf, 2016.

[6] R. Chigwin, "ICSA Labs wants IoT Industry to seek security certification: But will anyone care?," The Register, https://www.theregister.co.uk/2016/05/26/icsa_labs_wants_iot_industry_to_seek_security_certification, May 2016.

[7] AT&T, "The CEO's Guide to Securing the Internet of Things,"

Exploring IoT Security - AT&T Cybersecurity Insights, Vol 2, https://www.business.att.com/cybersecurity/archives/v2. 2016.

[8] S. Waterman, "Report: IoT devices attacked their own network," Cyberscoop, https://www.cyberscoop.com/verizon-2017-data-breach-digest-iot-devices-attack-network, Feb 2017.

[9] Icontrol Networks, "2015 State of the Smart Home Report Reveals Seeing is Believing, Smart Home Mass Adoption to be Led by Familiar Connected Products with Obvious Benefits," https://www.prnewswire.com/news-releases/2015-state-of-the-smart-home-report-reveals-seeing-is-believing-smart-home-mass-adoption-to-be-led-by-familiar-connected-products-with-obvious-benefits-300103481.html, Jun 2015.

[10] Federal Trade Commission. "Internet of Things: Privacy & Security in a Connected World," https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, Jan 2015.

[11] Nikos Vernardakis, *Innovation and Technology: Business and economics approaches*, Routledge, 2016.

[12] T.V. Krishnan, F.M. Bass, V. Kumar, "Impact of a Late Entrant on the Diffusion of a New Product/Service," *Journal of Marketing Research*, vol. 37, no. 2, pp. 269-278, May 2000.

[13] J.L. Bayuk, J. Healey, P. Rohmeyer, M.H. Sachs, J. Schmidt, J. Weiss, *Cyber Security Policy Guidebook*, Wiley, Chapter 6, Apr 2012.

[14] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf, Jan 2017.

[15] M. Scofield, "Benefiting from the NIST Cybersecurity Framework," *Information Management*, vol. 50, no. 2, 2016.

[16] D. Baer, "Your Office's Fluorescent Lights Really Are Draining Your Will To Work," Fast Company article, https://www.fastcompany.com/3005976/your-offices-fluorescent-lights-really-are-draining-your-will-work, Feb 2013.

[17] U.S. Energy Information Administration, "Commercial Buildings Energy Consumption Survey," Table B-6 and Table B-7, https://www.eia.gov/consumption/commercial, May 2016.

[18] U.S. Energy Information Administration, "Commercial Buildings Energy Consumption Survey," Table E-1, https://www.eia.gov/consumption/commercial/data/2012/c&e/cfm/e1.php, May 2016.

[19] M.S. Jalali, M. Siegel, S. Madnick, "Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment," *arXiv Preprint*, arXiv:1707.01031. 2017.

[20] S. Madnick, M.S. Jalali, M. Siegel, Y. Lee, D. Strong, R. Wang, W.H. Ang, V. Deng, D. Mistree, "Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems," *International Workshop on Data Analytics for Renewable Energy Integration*, Springer Cham, pp. 67-77, Sep 2016.

Mohammad S. Jalali is a research faculty at MIT Sloan School of Management. Dr. Jalali is interested in simulation and model estimation methodologies, and the applications of dynamic modeling for complex sociotechnical and organizational cybersecurity problems. He focuses his simulation modeling work on mechanisms that connect human decision making to sociotechnical systems, because that is where many important policy-resistant problems lie. Dr. Jalali also builds bridges across methodological and application domains and connects his mechanism-based models with big data. His work has been featured by various national and international media outlets, including Associated Press, Newsweek, and Business Insider. Dr. Jalali is a former consultant at the World Bank and a former researcher at the U.S. Department of Energy. He is also the recipient of the 2015 Dana Meadows Award, the 2015 WINFORMS Student Excellence Award, and the 2014 Lupina Young Researcher Award.

Jessica P. Kaiser is a Research Associate at the MIT Sloan School of Management. She is interested in technology risk management and has worked in data science and analytics in technology start-ups, including Rocket Fuel and Snapchat. She holds a B.A. in Mathematics from Northwestern University and an MBA from the MIT Sloan School of Management. She is the recipient of the Reaching Out MBA Fellowship and the Martin Trust Community Fellowship.

Michael Siegel is a Principal Research Scientist at the MIT Sloan School of Management. His recent research includes cybersecurity and critical infrastructure, modeling vulnerability markets, industrial control systems cybersecurity strategy and management, and the analysis of vulnerability markets. During his more than twenty-five years at MIT, Dr. Siegel's research interests have included the use of dynamic modeling and data mining for management and process improvement in critical systems, applications of computation social science to analyzing state stability and cyber security, digital business and financial services, financial risk management, value-at-risk benchmarking, heterogeneous database systems, managing data semantics, query optimization, intelligent database systems, and learning in database systems. Dr. Siegel has been active in research to improve cyber systems through, critical infrastructure analysis, simulating approaches to patching vulnerabilities, bug bounty programs and modeling of improvements to software development and maintenance. He is presently an Associate Director of Cybersecurity at MIT Sloan.

Stuart Madnick is the John Norris Maguire Professor of Information Technologies in the MIT Sloan School of Management and a Professor of Engineering Systems in the MIT School of Engineering. He has been a faculty member at MIT since 1972 and has served as the head of MIT's Information Technologies Group for more than twenty years. Dr. Madnick has been actively involved in cybersecurity research since 1979 and currently is the Founding Director of Cybersecurity at MIT Sloan. He has been active in industry, making contributions as a key designer and developer of projects such as IBM's VM/370 operating system and Lockheed's DIALOG information retrieval system. He has served as a consultant to major corporations and has also been the founder or co-founder of several high-tech firms. Dr. Madnick is the author or co-author of over 380 books, articles, or technical reports including the classic textbook, Operating Systems (McGraw-Hill), and the books, The Dynamics of Software Development (Prentice-Hall) and Computer Security (Academic Press). Dr. Madnick has degrees in Electrical Engineering (B.S. and M.S.), Management (M.S.), and Computer Science (Ph.D.) from MIT.