The Internet of Things 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

Working Paper CISL# 2019-06

March 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

The Internet of Things 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 | Sloan School of Management, Massachusetts Institute of Technology

Cyber risk for buyers is a major obstacle to broad adoption of the Internet of Things (IoT). Using a system dynamics approach, we conducted a case study of a connected lighting product to understand how cybersecurity influences IoT adoption.

The research in this article was conducted to better understand the mechanisms by which cybersecurity will influence IoT technology adoption. By focusing on innovation and marketing to power the growth of a product, there may be unintended consequences for security, such as leaving the product vulnerable to hacking. For developers, there is a strong tension between prioritizing product usability and product security, and their responses to the following questions about these new issues will shape the future marketplace. What standards will emerge for the IoT products? How will they prove their security to the market? Will a few key players dominate the market, or will it remain highly fragmented with a high firm entry and exit?

Despite the growing literature on cybersecurity, the direct mechanisms by which it may influence IoT adoption have not been studied. Given the IoT's unique vulnerabilities and relative infancy in the marketplace, it is unclear how a cyberincident could impact consumers' willingness to adopt it. Will IoT products experience the rapid "hockey stick" growth exhibited by tech companies such as Facebook? (See the green line in Figure 1.) On the other hand, could publicized cyberincidents hamper the growth of an IoT product to an extent that it never gets off the ground? (See the "Start-and-Fizzle" red dotted line in Figure 1.) Is the reality somewhere between these two extremes? (See the "Still Successful" and "Partially Successful" red dotted lines in Figure 1.) Also, will growth occur for the market as a whole, or will a few dominant players emerge? If the latter occurs, will those players be mature companies or start-ups? An example of a cyberincident's effect on product sales is the "My Friend Cayla" doll. After a feature of the doll (voice transmission to a U.S.-based voice recognition company) was found to be vulnerable to independent and possibly malicious hackers, it received a "trash it" recommendation from the German telecommunication regulator.[1]

We performed a case study of IoT product development for commercial building applications. Our subject was a connected lighting product at a large electronics company, which we analyzed using a system dynamics approach. This approach generates a framework that IT executives at supplier companies can use in strategic decision making to better understand what consequences—both intended and unintended—may arise from the

Digital Object Identifier 10.1109/MSEC.2018.2888780
Date of publication: 2 April 2019

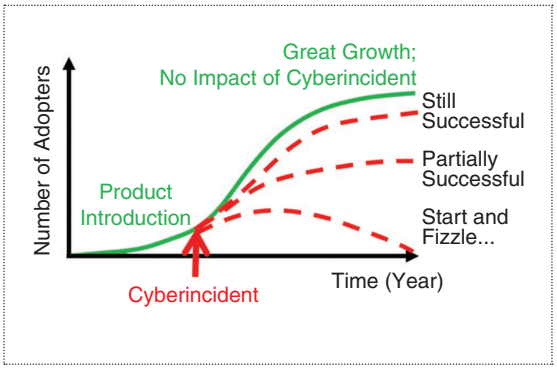

Figure 1. A range of product adoption curves in response to a cyberincident. A better understanding of how a breach may affect product adoption can guide managers who are making security investment decisions early in a product's development.

choices they make during IoT product development. We refer to customer organizations as *adopters* and organizations that produce IoT products as *suppliers*. 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., cyber risks), the initially successful strategies may not only become ineffective but may actually damage their position in the marketplace. Therefore, it is essential to take a systematic approach by looking at the big picture 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 we explored in our case study and model. We begin with an overview of the IoT. We then explain the basics of diffusion models, particularly the risk–reward ratio, a concept that our research showed to greatly influence IoT technology purchase decisions. Next, we describe current cybersecurity standards for technology purchase decisions. In the second section, we enter the case study, describing the IoT product market studied and then the model derived from our research and its implications. Four cybersecurity-related guidelines that managers can use to influence the market adoption of IoT products are included in "Cybersecurity-Focused Guidelines for Robust and Resilient Market Adoption."

Overview of Concepts

Introduction to the IoT

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

The goal of the IoT is to translate the physical world into digital signals, ripe for the improvements promised by faster communication and better analytics. Although there is no universally agreed-upon definition of the IoT, most definitions describe systems that collect data from the physical world on devices that process information.[2] The Internet society provides a good summary that explores the benefits and challenges of the IoT.[2] The digital processes are often intended to produce kinetic effects and rely heavily on networking with other external devices. Declines in the cost of computing and simultaneous improvements in sensor performance and range make innovations possible. There is a range of settings for which the IoT might be deployed, ranging from the intimate (i.e., personal health data) to the massive (i.e., a connected system of street lights, parking meters, transit, and autonomous vehicles that could be used to collect useful municipality data and optimize the delivery of city services to citizens). The potential value generated by the IoT is estimated to be at least US$3.9 trillion and possibly up to US$11.1 trillion by 2025, with the higher estimate representing 11% of projected global gross domestic product in the same year.[3]

> **One of the greatest obstacles to broad market adoption of IoT technology is the buyers' fear of cyber risk, both real and perceived.**

One of the greatest obstacles to broad market adoption of IoT technology is the buyers' fear of cyber risk, both real and perceived. The Open Web Application Security Project[4] described IoT technologies as having three unique weaknesses with regard to cybersecurity: a large number of endpoints, inconsistent protocols, and physical safety concerns. There are currently no mechanisms that could manage consistent endpoint security for a system that is so vast. Additionally, the diversity of standards across the IoT defrays the responsibility of any single actor in the technology chain for security. As of now, there are two commercially available certification programs for IoT security, one from Underwriter Laboratories and one from ICSA Labs, an independent division of Verizon (New York). Both were launched in 2016 and have been met with some skepticism, as noted in an article in *The Register*.[5] Because the IoT represents a linked

Cybersecurity-Focused Guidelines for Robust and Resilient Market Adoption

To increase their market size and keep their market resilient to cyberincidents, Internet of Things (IoT) product managers should consider these four guidelines, which we have compiled through our case study partner and which were built by our model.

1. *Invest in cybersecurity capabilities from product design to sales to ongoing support*: Cybersecurity expertise is required not only to build security products and processes, but to explain it to customers. As cybersecurity becomes a top-of-mind concern for most customers, it will become more important to have cybersecurity experts at every customer touchpoint. These experts can address concerns, prevent and detect threats, and respond to incidents. Additionally, organizations must have a detailed incident-response plan with clear actions and owners. Make sure transferring ownership is a part of succession planning and conduct regular reviews of the response plan to ensure that it remains up to date.
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 developers to understand the potential impact of a cyberincident on market adoption. It can also guide investment decisions as you develop the product or its new features. The risk–reward ratio of IoT products has a dynamic mechanism and changes over time, so be sure to measure and monitor it regularly.
3. *Capture data at the granularity level that shows measurable benefits for customers, and no lower*: The benefits of many IoT technologies cannot be fully realized without granular data capture and processing. If it is too granular, however, two things happen: 1) cyber-risk exposure increases considerably and 2) the product's benefits become more difficult to understand and capture. In both cases, market adoption slows. When expanding into new market features and more granular data is required, partner with firms with strong analytic capabilities and data-protection practices for case studies that show measurable benefits.
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 that has a reputation for strong security. If you develop your own platform, work with third-party companies to certify its safety. If creating hardware, buy it 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.

set of physical devices, it gives malicious actors the opportunity to move their criminal activities—previously confined to cyberspace—into the physical world.

These characteristics of IoT cybersecurity are not merely pedantic; they are being exploited. A large-scale, distributed denial-of-service (DDoS) attack that took place in 2016 exemplifies this exploitation. In the time leading up to the attack, AT&T tracked a 400% increase in scans of IoT ports and protocols.[6] 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 a large quantity of nodes are used to overwhelm a network with traffic.

Finally, both individual and organizational adopters of the IoT have concerns about its security and privacy implications. The 2015 Icontrol State of the Smart Home study found that more than 40% of Americans were very concerned about the possibility that their information could be stolen from their smart homes.[7] Furthermore, potential regulators in the Federal Trade Commission have noted that such concerns may prevent IoT technologies from reaching their full potential, although it is not clear how these concerns alter consumers' purchases.[8] In industries that have an increased exposure to technology, such as banking, defense, and health care, security concerns are heightened.

Basics of the 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 with product adoption. The S curve describes how the user base is small to start, then increases as adoption increases, and eventually approaches the limit of the potential market.

It has been observed in the diffusion of many diverse innovations, such as electricity, the washing machine, and most recently social media networks such as Facebook (shown with the green line in Figure 1).

Vernardakis[9] grounds the underlying Bass diffusion model on an understanding of the diffusion process as an epidemic. The innovation spreads through information exchange, and the 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 that includes the awareness, consideration, opinion formation, and implementation phases.

A crucial variable in diffusion models is the speed of diffusion, which several factors affect. A critical factor that affects 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 number of potential adopters is another such factor as a larger number creates more opportunities for sharing information about the innovation. The information channels and the supplier's ability to affect these channels also are powerful forces affecting information transmission.

A feature of the Bass diffusion model is that it leads to "winner-take-most" scenarios because only an information exchange is needed to catalyze the innovation adoption process. Systems scientists have defined *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. Standards play an important role in innovation diffusion because they demonstrate that a product is compliant, and compliance reduces the friction and delays that would otherwise present themselves during the opinion formation stage. Many supplier companies compete to become the standard in their industry and thus reach the tipping point.

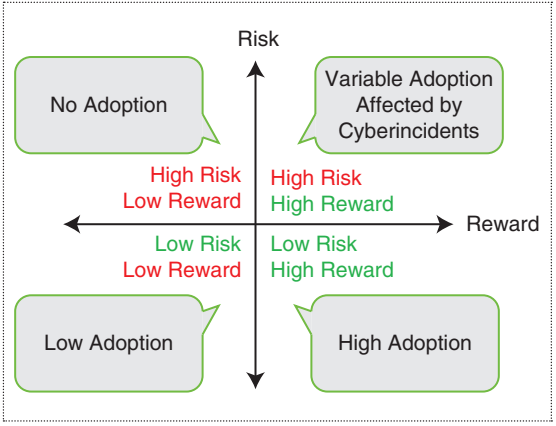

Figure 2. The adoption of the IoT based on risk and reward.

Krishnan et al.[10] show that additional products entering an innovation marketplace late can increase the speed of diffusion, although the evidence is mixed with regard to how it impacts the incumbent's market share. For start-ups, this is a powerful incentive to enter the marketplace as a small start-up 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 in regard to developing standards. It might be better to achieve immediate revenue by adopting another company's standard and reducing decision friction for customers. However, if a firm can create its own standards, it might be able to prevent other firms from entering the marketplace and thus reduce competitors' market share.

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

"[Cybersecurity] is more a concern for late-majority adopters." —Product manager

Within the context of IoT technologies, a product gains an advantage if connecting an object to a network improves the adopter's operations. The data that IoT devices produce is often what creates the relative advantage. In our research, we call this the *risk–reward ratio*, noting that as the granularity and utility of data produced by an IoT product increase, 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 because some data must be better than no data. However, not every IoT product is adopted as quickly as expected. Although many individuals are installing connected thermostats, few are connecting their microwaves, and connecting stove knobs is unheard of despite the benefit that acquiring cooking data could bring. As we will explore, in the case of commercial building operators, businesses have adopted connected heating, ventilation, and air-conditioning (HVAC) systems more quickly than they have adopted connected lighting, despite the cost-savings benefits across both products. Therefore, it must be the case 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 could be in plumbing or in physical security. Connecting these infrastructures can provide multiple benefits, most frequently the central control and visibility that allow building managers to manage their use and maintenance more efficiently. We will discuss more benefits for connected lighting systems (CLS) in particular over the course of this article. We summarize the effects of the risk–reward ratio on adoption in Figure 2 and discuss this framework more in our case study in the "Adoption of Connected Lighting Systems" section.

Cybersecurity Standards in Technology Adoption Decisions

It is valuable to review how practitioners assess the security risk in technology when making purchasing decisions. However, because cybersecurity as a discipline is evolving rapidly, practitioners have not yet arrived at consistent, universal standards for evaluating cybersecurity risks. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, born out of a 2013 Executive Order and now in Draft Version 1.1, is the leading framework that has emerged. It provides high-level direction on steps that organizations should take to improve cybersecurity iteratively, steps that an organization would use to adopt a new technology. They roughly align with the adoption process that we discussed in the "Basics of the Diffusion Model of Technology" section.

One critique by IoT adopters is that no standards currently define the market. Suppliers, however, have a mixed perspective. Although the lack of standards is a possible strategic advantage, particularly for start-ups because it is easier to enter the market, the lack of standards also makes it difficult to articulate to adopters how to manage cyber risk. The NIST framework is technology neutral precisely because no standards yet exist. The government has been ineffective in 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, before the winner-take-most effect takes hold in the marketplace. The current market presents a potentially lucrative opportunity for IoT suppliers, start-ups, and incumbents alike.

Adoption of Connected Lighting Systems

Case Study Approach to Effects of Cybersecurity on CLS Adoption

"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

Although there is research on cybersecurity, the IoT, and technology adoption individually, research that articulates how each contributes to overall market adoption is lacking. In this article, we approach cybersecurity and IoT adoption from a systems science perspective. We interviewed practitioners from the security, product, marketing, and sales departments of a large electronics company that produces an IoT lighting product. We also interviewed 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 a comparison of the risk–reward ratios for both products, we use their responses to adjust the typical Bass diffusion model to include cybersecurity-related variables. Next, we use this model to articulate implications that reflect what impact cyberincidents may have on an IoT product market. Finally, we encourage managers to adopt IoT products by using these implications to outline four cybersecurity-related guidelines.

CLS: Product Benefits

"People are clear on the rhetoric of IoT, but not what value it delivers." —Manager for lighting products

CLS are one of a few building infrastructures that can be transitioned to the IoT because: 1) they are a point of frequent interaction for building occupants; 2) there is a large number of nodes, and light bulbs are good candidates for granular data collection; and 3) there is an opportunity for personalization as lighting preference is highly individualized. 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. Two examples are occupancy sensors and LED light bulbs. Occupancy sensors turn lights on and off only when they are needed, without end-user intervention, and LED light bulbs require little maintenance.

When describing the benefits of CLS, interviewees used the "US$3–US$30–US$300 rule" to describe the value opportunity of CLS. No external source was found to validate this rule. Connecting lighting alone represents an energy-efficiency cost-savings opportunity of only US$3 per square foot per year, but space optimization represents US$30 and employee productivity is an additional US$300 cost per square foot per year savings opportunities. This rule is derived from ex post facto analysis and has not been verified empirically.

Connected light bulbs can detect that a company uses a conference room only 20% of the time while employees use desks outside the conference room 100% of the time. These data could signal that the space is underoccupied and that they could use the conference room space more efficiently. Also, consider an office building that has an "open desk" policy, in which employees are not assigned to desks and can use any open space. Motion sensors on light bulbs can detect which desks employees are using, allowing IT systems to direct employees to an available desk when they enter the building. Practitioners believe that occupancy data and space-saving systems such as these represented a US$30 per square foot per year cost-saving opportunity.

The ultimate goal of CLS for commercial applications lies in collecting data about productivity that occurs under

the light bulbs. Practitioners note that lighting has a strong physiological and psychological effect on workers, so a CLS could adjust the hues and saturation of light to create a personalized environment to complement an employee's work style and thus generate additional productivity for a firm. If implemented correctly, interviewees believe that this application represents an enormous cost-savings opportunity of US$300 per square foot per year.

For home rather than business adopters, the US$3–US$30–US$300 rule is believed to apply directionally. However, adopters are unlikely to attempt to justify their purchase by quantifying the benefits without the resources of a larger organization. Instead, the product's relative advantage depends on how important customizing lighting hues and saturation in a home environment is to a customer. Given the lack of case studies or empirical data supporting the rule, the underlying theory has not been proven and makes the relative advantage of CLS confusing to both home and business adopters.

The confusion regarding the benefits of CLS is in contrast to connected HVAC systems, another building system that has been connected to the IoT. When compared with HVAC systems, which represent about 44% of energy costs in commercial buildings, lighting systems represent about only 10% of a building's energy costs.[12] Because HVAC systems contribute such a large portion of a building's energy bill, and components such as chillers are more expensive to maintain proactively, connecting HVAC systems to the IoT presents immediate and easily quantifiable benefits to the adopter. Interviewees felt that the rewards of connected HVAC systems are easy to measure. This 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.

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

When describing the features of CLS most often considered prior to adoption, an important yet confusing aspect is its "cybersecurity" component. 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 1 for a list of features and their achievements across CLS.) We propose four possible explanations for 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), which makes 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 US$100 for a light bulb, versus thousands of dollars for a chiller).
3. Potential adopters did not have the internal analytic capabilities, including sufficient data security and

Table 1. Feature-exploit analysis of connected building infrastructure (e.g., CLS and HVAC).

Feature	Value	Exploit
Personalization (e.g., color or temperature control)	Greater occupant satisfaction and productivity	Ability to create annoyance, harassment, or physical discomfort Ability to overload output for physical damage
Wireless control system	Insight into energy, occupant utilization, and component use Integration to improve efficiency and occupant satisfaction	Ability to access core IT for espionage or use in illegal activities Packet sniffing, replay, trashcan, social engineering, and others
Central and local control	Balance between energy use and occupant comfort Greater ease of use	Potential for DDoS attacks through nodes Opportunity to sabotage or interfere with operations through ransomware
Occupancy sensor	Greater ease of use Space optimization Coordinated responses Energy efficiency	Passive surveillance Maximization of damage during kinetic attacks Minimized risk of being caught (e.g., burglary)
Power over Ethernet	Lower installation costs Energy reporting	Potentially easier to disrupt Limited security literature

Only the power over Ethernet is unique to CLS.

privacy protection, to leverage the space optimization and productivity benefits of CLS.

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 intimately personal data on an IoT device. However, when the IoT device processes personally identifiable information or medical data, the risks for physical harm beyond discomfort increase.[13]

The "Iceberg" Model

Presentation

"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

Regardless of their size, most supplier companies that produce new technologies create innovations that they believe present a possible solution to a customer's pain point. They test early versions of the product to gauge whether they are attractive to customers and, if they are, use market growth to drive product improvements. This cycle is represented by the blue feedback loops in Figure 3.

If consumers find the product attractive, then its adoption will increase. The positive sign on the arrow represents that the two variables change with the same polarity, either an increase in the attractiveness causes an increase in the adoption or a decrease causes a decrease. As the rate of adoption of IoT increases, the number of adopters of IoT also grows, gradually increasing the size of the product's market and producing more revenue for the company. Collectively, the supplier company receives enough revenue to reduce the price, increases research and development, improves the technology, and makes it easier to use. This process in turn makes the product even more attractive (completing the three loops in Figure 3) and brings in even more customers. If the supplier company can activate these reinforcing cycles, then they can reach the tipping point and generate the steep growth of the S curve that was explored earlier in this article.

As the iceberg 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 other factors beyond "success begets success" influence the information-gathering and opinion-formation phases of the adoption cycle. In our case study, several internal experts and potential adopters mentioned cyberincidents and the cybercriminal market when discussing the product's risks, which is suggestive of the cycle presented in Figure 4. Cybersecurity elements could act as a balancing force to the other adoption mechanisms in both the adopter's and the supplier's direct control.

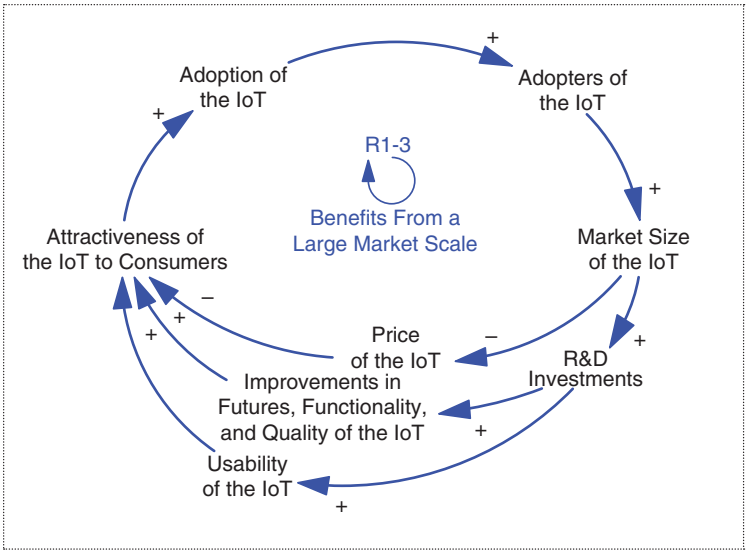

Figure 3. The visible "tip of the iceberg" or how market adoption benefits product development.

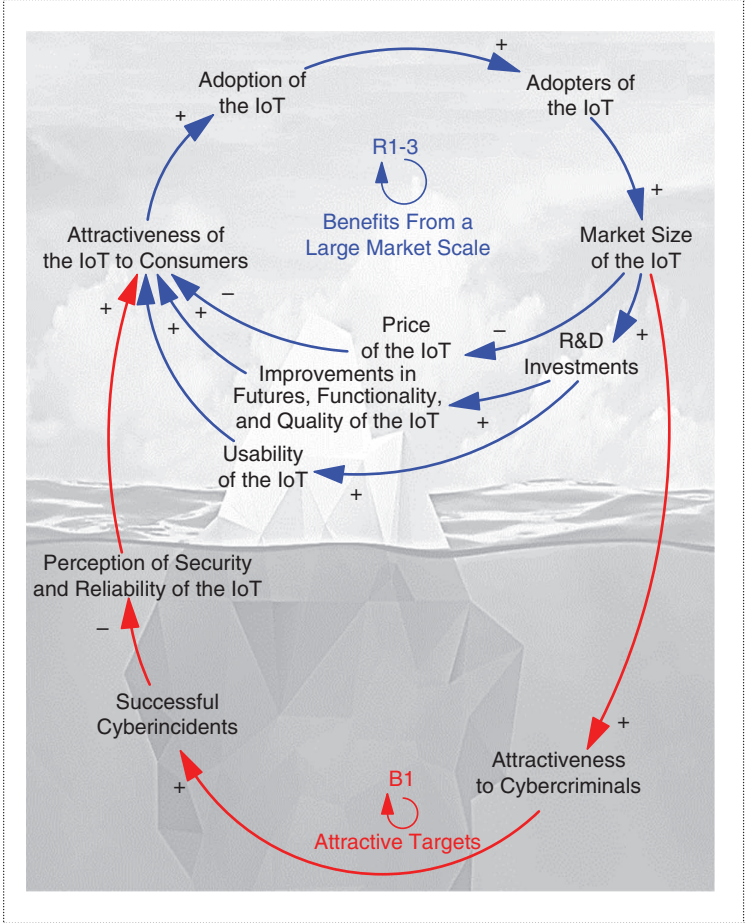

Figure 4. The "iceberg" model. The balancing feedback loop (B1) works against the reinforcing loops (R1-3) to limit the product's potential growth but is not necessarily visible to product managers unless they experience a cyberincident.

In the model presented in Figure 4, 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 customers learn about the attacks, the perceived security and reliability of the product will diminish (as shown in the balancing loop labeled "Attractive Targets" in Figure 4). Although a supplier company is focused on introducing additional features, potential adopters may decide that the cyber-risk exposure is too great to justify the product's benefits or any number of novel features. Thus, the activity of the cybercriminal market, shown in red in Figure 4, becomes a countervailing force on the activities of the manufacturer, shown in blue.

Implications

"You can spend 15–20 years building up your brand, and a cyber attack can crush it in two or three minutes." —an interviewee

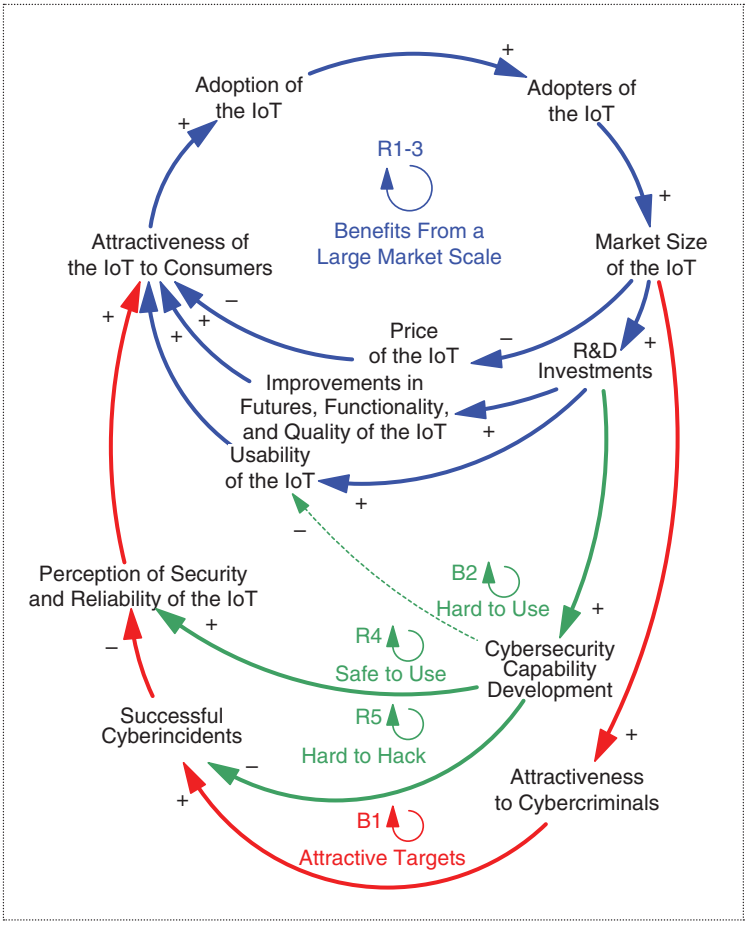

Figure 5. The developers fighting back. To limit the effects of the cyberincident's balancing loop (B1), product developers must also invest in developing cybersecurity capabilities.

The counterforce mechanism of cyber criminal activity on market adoption (the red loop in Figure 4) may slow the adoption of IoT products, which explains 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 with HVAC products, despite the well-publicized HVAC cyber achievements. The cost-saving opportunities of CLS products in the space optimization and productivity categories have not been fully realized because most adopters are still building internal analytic capabilities, so only the smaller benefits of energy efficiency are immediately recovered by adopters. A cyberincident targeting CLS this early in its adoption cycle could have a big impact on the market.

Cybersecurity Capability Development

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

Consider an example of two hypothetical IoT supplier start-ups: one chooses to invest in cybersecurity capabilities as it begins to grow, whereas the other does not. As their market size grows to a scale that makes them attractive to cyber criminals, the organization that invested in cybersecurity is less likely to receive a cyber attack and will ultimately be more successful, based on their reputation for security and reliability (see Figure 5, loop R5, "Hard to Hack"). Developed cybersecurity capabilities can also influence consumers' perception of security and reliability of the product, which eventually helps to increase the adoption of IoT (see Figure 5, loop R4, "Safe to Use").

In Figure 5, the place where the green and blue loops come into tension shows improving the product's usability. Security features are often seen by customers as inconveniences (see loop B2, "Hard to Use"). In an IoT context in which technology's usability may be critical for ensuring ongoing business operation and success in the market, it may be attractive for manufacturers to avoid security features such as two-factor authentications or even simple password requirements. However, increased cyberincidents would soon result in customers no longer perceiving the product to be secure or reliable. The product must be simple enough to attract customers, yet secure enough to reduce the likelihood of successful cyberincidents. For IoT products, which are similar to IT products in general, this tension between usability and security must be resolved between the purchasing company's different departments. Typically, the IT department outlines acceptable security guidelines. However, IT is not the department that mainly

understands the core use cases that make CLS attractive to purchase. As a result, IT and the potential CLS purchaser must be able to resolve these issues as part of the deployment and installation process. Our interview subjects described the importance of navigating an organization during the sales process. By determining who in the organization was responsible for cyber risk, and involving them in the purchasing process, the product met all cybersecurity protocols. Moreover, our case study partner made additional investments to increase the cybersecurity domain knowledge of their salesforce, to ensure that their sales force had the skills needed to identify both IT and operational cyber risk and to facilitate productive dialog between IT and the CLS purchaser.

In a large, resource-rich organization, investing in cybersecurity capabilities might mean prioritizing security during resource allocation, as well as working to become the standard for security in the IoT industry, to get closer to the tipping point. A resource-scarce organization, such as an IoT start-up struggling for cash, people, and time, faces a tradeoff. Managers could focus on reaching the tipping point to achieve stable revenues that can be invested in security (and risking attack along the way). Alternatively, they could focus on security right away, at the expense of attracting early customers. Jalali et al.[14] show that overcoming decision-making biases when building cybersecurity capabilities is difficult even for experienced managers. Furthermore, it is not clear whether perception and reality are well aligned when it comes to security. In Massachusetts Institute of Technology's "House of Security" study, executives demonstrated a significantly lower ability to assess their organization's vulnerability relative to low- and mid-level employees.[15]

Our case study partner can provide a general example of developing cybersecurity capabilities in the early stage of product adoption. This company chose to invest its resources in the following ways.

- *Practice secure lifecycle development*: Including both secure coding practices and clear guidelines regarding third-party vendor evaluation and factory disposal practices, the goal is to provide the firm with clear and consistent cybersecurity best practices throughout the product's lifecycle. One practice that the firm thought was important for identifying potential risks in the early adoption stages (i.e., after development is completed) was to ensure that new products underwent an extensive external penetration test prior to market release. However, continuous testing throughout the development stage is essential.
- *Develop cybersecurity thought leadership through customer relationships*: In an attempt to position the company as a secure vendor and to improve its cybersecurity practices, our research partner worked with its customers to identify and share cybersecurity practices. In cases when customers did not have strong cybersecurity practices, the company would work with them to provide training and education. As they are still early in the process of developing IoT products, they are still learning what the risk areas are, for both the IoT broadly and their CLS product in particular. As a result, these customer forums provide not only valuable learning for customers, but also insights that the supplier can bring back to the product-development stage for both CLS and future IoT products.

It should be noted that the two practices discussed here are only examples of cybersecurity capability development and are not meant to be comprehensive.

Our model contributes to the diffusion literature by introducing consumers' perception of security and reliability as a major driver for adoption. Interviews showed that firms have not yet developed best practices to rigorously measure and manage that perception. For instance, although the risk–reward ratio drives CLS adoption, the firm in question had only just begun to discuss how to measure it. One potential direction is to leverage firms' developing interest in cybersecurity thought leadership to survey their customers regularly about their perception of the risks and rewards of CLS. This continuity-of-survey analysis is particularly important because: 1) the cybersecurity risks of IoT products are not solely determined at the product-development stage, but may emerge or be affected when the adopters deploy them into different ecosystems and 2) perceived risks and benefits are a dynamic mechanism that can change over time, so a one-time survey does not provide enough information. A next step in understanding IoT adoption for any product, including CLS, would be to measure the risk–reward ratio rigorously as the information-security and risk-management literature provides more information about this measurement.

Our model also presents some interesting questions for future research. For example, would it be possible to quantify how attractive the market is from criminals' perspectives? How do areas that focus on cybersecurity capability shift development as a product moves through different stages of market adoption? How might a supplier firm quantify the impact of cybersecurity on the price or utility? Future work would aim to quantify the variables presented in the adjusted model in order to generate answers to these questions.

Acknowledgments

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 allowed us to interview them for our research. We appreciate their time and expertise in building and validating this model. Cybersecurity at MIT Sloan (CAMS) provided financial support for this study. ■

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," 2015. [Online]. Available: https://www.internetsociety.org/resources/doc/2015/iot-overview
3. J. Manyika et al., "Unlocking the potential of the Internet of Things," McKinsey Global Inst., June 2015. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
4. Open Web Application Security Project, "Internet of Things (IoT) Project," 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
5. R. Chigwin, "ICSA Labs wants IoT industry to seek security certification: But will anyone care?" *The Register*, May 2016. [Online]. Available: https://www.theregister.co.uk/2016/05/26/icsa_labs_wants_iot_industry_to_seek_security_certification
6. AT&T, "The CEO's guide to securing the Internet of Things. Exploring IoT security," *AT&T Cybersecurity Insights*, vol. 2. [Online]. Available: https://www.business.att.com/cybersecurity/archives/v2. 2016.
7. 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," Jun. 2015. [Online]. Available 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
8. Federal Trade Commission, "Internet of Things: Privacy & security in a connected world," Jan. 2015. [Online]. Available: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
9. N. Vernardakis, *Innovation and Technology: Business and Economics Approaches*. New York: Routledge, 2016.
10. T. V. Krishnan, F. M. Bass, and V. Kumar, "Impact of a late entrant on the diffusion of a new product/service," *J. Marketing Res.*, vol. 37, no. 2, pp. 269–278, May 2000.
11. U.S. Energy Information Administration, May 2016. "Commercial buildings energy consumption survey, Table E-1." [Online]. Available: https://www.eia.gov/consumption/commercial/data/2012/c&e/cfm/e1.php
12. U.S. Energy Information Administration, May 2016. "Commercial buildings energy consumption survey, Table B-6 and Table B-7." [Online]. Available: https://www.eia.gov/consumption/commercial
13. M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J. Medical Internet Res.*, vol. 20, no. 5, Art. no. e10059, May 2018.
14. M. S. Jalali, M. Siegel, and S. Madnick, "Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment," *J. Strategic Inform. Syst.*, Sept. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0963868717304353
15. S. Madnick et al. "Measuring stakeholders' perceptions of cybersecurity for renewable energy systems," in *Int. Workshop on Data Analytics for Renewable Energy Integration*. Cham, Switzerland: Springer, 2016, pp. 67–77.

Mohammad S. Jalali was a research faculty member at Sloan School of Management, Massachusetts Institute of Technology when this study was conducted. His research interests include simulation and model estimation methodologies and the applications of dynamic modeling for complex sociotechnical and organizational cybersecurity problems. He received the 2015 Dana Meadows Award, the 2015 WINFORMS Student Excellence Award, and the 2014 Lupina Young Researcher Award. Contact him at jalali@mit.edu.

Jessica P. Kaiser is a research associate at the Sloan School of Management, Massachusetts Institute of Technology (MIT). Her research interests include technology risk management. Kaiser received an M.B.A. from the Sloan School of Management, MIT. She received the Reaching Out MBA Fellowship and the Martin Trust Community Fellowship. Contact her at jpkaiser@mit.edu.

Michael Siegel is a principal research scientist and associate director of cybersecurity at the Sloan School of Management, Massachusetts Institute of Technology. His research interests includes cybersecurity and critical infrastructure, modeling vulnerability markets, industrial control systems cybersecurity strategy and management, and analysis of vulnerability markets. Contact him at msiegel@mit.edu.

Stuart Madnick is the John Norris Maguire Professor of Information Technologies at the Sloan School of Management, Massachusetts Institute of Technology (MIT) and a professor of engineering systems in the MIT School of Engineering. Madnick received a Ph.D. in computer science from MIT. Contact him at smadnick@mit.edu.