Government Information Quarterly 35 (2018) 151–160

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets

Zhen Li[a], Qi Liao[b,*]

[a] Department of Economics and Management, Albion College, USA
[b] Department of Computer Science, Central Michigan University, USA

ARTICLE INFO

Keywords:
Smart cities
E-government
Cybersecurity
Vulnerability
Economics
Game theory

ABSTRACT

Cities are becoming smarter and smarter. While the rapid progress in smart city technologies is changing cities and the lifestyle of the people, it creates also huge attack surfaces for potential cyber attacks. The potential vulnerabilities of smart city products and imminent attacks on smart city infrastructure and services will have significant consequences that can cause substantial economic and noneconomic losses, even chaos, to the cities and the people. In this paper we study alternative economic solutions ranging from incentive mechanisms to market-based solutions to motivate governments, smart product vendors, and vulnerability researchers and finders to improve the cybersecurity of smart cities and e-government. These solutions can be integrated into policy instruments in defending smart cities and e-governments against cyber attacks.

1. Introduction

Cities are getting smarter and smarter in recent years. Communities around the world, from small towns to big metropolitan areas, are turning to modern technologies to connect government agencies and citizens to deal with urban problems such as traffic congestion, public service shortcomings, and energy shortages. To ensure the efficiency and effectiveness of providing public services to people, the smart city concept requires bringing together various information and communications technologies and solutions. While technologies are changing cities and the lifestyle of the people, the rapid growth of smart cities and e-government is also posing enormous challenges in terms of the safety and security of the cities. One specific concern is the safety of smart city products themselves. The potential vulnerabilities of smart city devices and systems largely result from the inherent vulnerable characteristics of these products as well as the lack of incentives in the design and implementation of security features of these products. As smart city infrastructure development outpaces cybersecurity solutions, smart software, devices, and systems are vulnerable to intrusion and malicious cyber attacks.

In smart cities, cybersecurity plays the key role in protecting availability, integrity, stability, as well as the confidentiality required to support smart environments. Cybersecurity used to be seen as purely a technical problem. Researchers and practitioners largely depended on technologies for cybersecurity solutions. Nevertheless, humans are players in every cybersecurity attack-defense game. It is informative to study the motives of each interested party involved in the cybersecurity issue and design corresponding non-technical solutions to reduce cyber attacks. In the cybersecurity game of smart cities and e-government, there are at least four types of stakeholders involved: governments, smart solution providers, vulnerability finders, and cyber attackers. It is important to study the incentives and interdependence of various stakeholders' decision making. This paper focuses on feasible economic solutions to enhance the cybersecurity situation of smart cities and e-government by analyzing incentives, especially financial incentives, of the stakeholders' behaviors and interactions during the process of building and managing smart cities.

The main contributions of this study are twofold. First, we formally model the life cycle of smart city vulnerabilities by considering the role of government, smart product vendors, internal vs. external vulnerability finders, and offensive vs. defensive vulnerability buyers, as well as the likelihood of malicious cyber attacks on smart cities and e-government. The model is further analyzed in a four-party game theoretical framework. Second, two alternative economic solutions are proposed based on the modeling analysis of economic incentives. The first proposal is carrot-and-stick-like strategies, i.e., the government either rewards the product vendor for security investment by paying a security premium on smart city products or holds the vendor accountable for product vulnerabilities and punishes the vendor financially for vulnerability exploitation. The second proposal is to encourage smart product vendors and governments to participate actively in the vulnerability market and compete with malicious attackers to acquire

* Corresponding author at: Department of Computer Science, Central Michigan University, Mount Pleasant, Michigan 48859, USA.
E-mail address: liao1q@cmich.edu (Q. Liao).

http://dx.doi.org/10.1016/j.giq.2017.10.006
Received 18 October 2016; Received in revised form 9 October 2017; Accepted 12 October 2017
Available online 28 October 2017
0740-624X/

vulnerabilities for defensive purpose.

The rest of the paper is organized as follows. Section 2 discusses related work and how this study fits in the literature. Section 3 discusses potential vulnerability of smart cities to cyber attacks and how dual disincentives existing in product development and implementation may lead to lack of security in smart city products. Section 4 uses a life cycle model of vulnerability to study the relationship between government, smart product vendors, vulnerability finders, and vulnerability exploiters. It identifies key factors that determine the chance of cyber attacks on smart cities. Section 5 proposes two economic mechanisms to improve security situation of smart city systems. Policy instrument design, limitation of this study, and future research avenues are also discussed. Section 6 concludes the paper.

2. Related work

Interest in the concept of smart cities has been expanding in recent years since it was first studied in the 1990s (Cocchia, 2014). There exists a large literature on the implementation of smart city concept and the around-world practices of making cities smart (Sureshchandra, Bhavsar, & Pitroda, 2016). They address shortcomings, challenges and risks with smart city initiative, and give practical suggestions. It has been argued that smart city thinking and initiatives need to be reframed in several ways, including normative and conceptual thinking with regards to goals, cities and epistemology, and practical and political thinking with regards to management/governance, ethics and security, and stakeholders and working relationships (Kitchin, 2016).

Smart urban services depend on mobile communications. The increasing potential benefit from the vulnerability exploitation in the mobile system has attracted significant attention from the black market (Algarni & Malaiya, 2014). While Android continuously increases its popularity in the mobile ecosystem, compared to other vulnerabilities, the vulnerabilities in the Android market are more exploitable, possibly due to the fast growing number of apps (Huang, Zhang, Tan, & Feng, 2015). Android apps have been found to have substantial software reuse, and the quality of the apps and libraries reused determines the quality of the apps (Mojica et al., 2014).

Security is essential to the success of smart cities and e-government because it determines users' incentive to use government services (Alsultanny, 2014, September-October). The ability to measure the quality of a technology is a prerequisite to obtain a high quality service, but it is hard to evaluate the quality of the services e-governments provide to users in all the management, information, service, and technical domains (Sa, Rochac, & Cota, 2016). Governments' lack of ability to frame cybersecurity can lead to the failure of developing suitable security policies (de Bruijn & Janssen, 2017). Considering the way humans, government, and technology interact, security education is desirable to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues (de Bruijn & Janssen, 2017; Klaper & Hovy, 2014). As cybersecurity specialists are found to overdramatize or over-simplify cybersecurity risks with management guru techniques, there is also a need for government to validate those statements (Quigley, Burns, & Stallard, 2015). A report outlined common risks that come with technologies adopted by local governments, and provided a *Best Practices and Resources Guide* local governments can use to achieve technology proficiency (Pfeiffer, 2015).

Usual cyber security technologies and best practices are necessary to protect smart city devices and systems. Studying the life cycle of vulnerabilities helps vendors reduce potential vulnerabilities during the software development process (Bilge & Dumitras, 2012), but technologies are only part of the solution. Technical advancements within software design and development have not prevented the release of insecure software and consequently the appearance of vulnerabilities and occurrence of exploitation. Depending on layers of walls difficult to breach to create security is outmoded for cybersecurity (Leuprecht, Skillicorn, & Tait, 2016). Economic, political, and other non-technical incentives are increasingly perceived as the primary reasons for today's increased risk exposure. Non-technical approaches need to be explored.

Software vulnerability disclosure is found to force vendors to release patches (Arora, Telang, & Xu, 2008). It may also affect the volume of attacks (Arora, Nandkumar, & Telang, 2006). Economics-based mechanisms of vulnerability disclosure, such as vulnerability reward program, can be effective to restrict the diffusion of vulnerability exploitation (Ransbotham, Mitra, & Ramsey, 2012, March). Study of Google's experience with its vulnerability reward programs (Mein & Evans, 2011, March) and a comparative research on two vulnerability reward programs by competing browser vendors, Google Chrome and Mozilla Firefox (Finifter, Akhawe, & Wagner, 2013) found reward programs economically beneficial to vendors. The government may create legal protections for cybersecurity research and enhance financial incentives to limit the supply of software vulnerabilities to attackers (Herr, 2017). It has been proposed to create an international vulnerability purchase program in which the major software vendors would be induced to purchase all of the available and known vulnerabilities at prices well above the black market prices (Frei & Artes, 2013, December).

There has been rising attention paid to cybersecurity of smart cities and e-government. Issues studied include the protection of citizen's privacy and personal data (Belanche-Gracia, Casalo-Arinob, & Perez-Rueda, 2015; Wu, 2014), security of e-government websites (Zhao & Zhao, 2010), and security of governmental use of cloud computing (Paquette, Jaeger, & Wilson, 2010). Economic mechanisms were proposed to improve smart city cybersecurity (Li & Liao, 2016). As consumers of smart city technology and policy maker, the government's potential to create economic incentives with policy making has not been fully addressed in the context of smart cities and e-government. This study extends existing work and further discusses economic solutions that can be disengaged into working policy instruments in defending smart cities and e-government against cyber attacks.

3. Security implications of smart cities

In this section, we discuss the potential vulnerability of smart cities to cyber attacks and the existing lack of security consciousness in the design and adoption of smart city products.

3.1. Cyber attack threat on smart cities

Smart city technologies are backed up by data collection and sharing, machine to machine communications, Internet of Things (IoT), and city management systems. Conventional cybersecurity issues apply to smart city technologies as well. Smart cities may be even more vulnerable to cyber attacks.

First, smart cities rely on wireless and mobile technologies for providing services. Wireless networking sets the communication infrastructure required for connecting smart objects, people, and sensors together, and allows for new capacities such as real-time monitoring and coordinating. For instance, many cities use wireless technology for their security cameras and infrastructure, rather than the hard-wired setups common in the past. This shift from wired to wireless networks makes things more cost and time effective for cities, but compared to hardware systems that were only physically accessible, remote attacks become possible on systems software controlled and remotely accessible.

Second, the information technology infrastructure of smart cities is different from other entities. A smart city ecosystem is a widely interconnected network, much bigger than any regular system of a private organization such as a business. It features complex interdependence between agencies and infrastructure, all working together to keep cities as a whole functioning properly. For example, smart payment terminals are commonly used at train stations, parking garages, etc. that process user information. They are connected to each other, run 24/7, and may

have access to other local area networks. With such interconnection and availability, it is hard to know what is exposed and the level of exposure. Attackers have many potential ways to interfere with the services.

Third, smart cities use latest technologies and development in information collecting, processing and communicating. The number of new devices used is gradually growing. These new devices are connected to existing devices and systems. For this ever-evolving environment to be resilient to cyber attacks, new products shall be added with caution. Nevertheless, the development in devices is faster than the development of security tools.

Smart city devices and systems could be easily hacked. Smart products often have the same configuration across devices of the same type. An adversary can control traffic infrastructure to cause disruption (Ghena, Beyer, Hillaker, Pevarnek, & Halderman, 2014). Major security weaknesses have been revealed in smart power meters (Illera & Vidal, 2014). Cities could be vulnerable even when nobody is actively hacking the smart systems. There have been numerous examples of cascading failures caused by system malfunctions, natural disasters, or industrial accidents such as the Northeast blackout of 2003 and the shutdown of San Francisco Bay Area Rapid Transit in 2013, both caused by software bugs. Just like a single bug could have drastic impact on a city running critical services on a large number of devices and systems, vulnerability exploitation would have similar consequences.

While smart cities have not yet become major targets of cyber attacks, threats are becoming real, both technically and intentionally. Large-scale attacks are not a matter of *if* but *when*. On the one hand, exploitation of mobile devices are overblown (Brumfield, 2015), and will continue to be growth areas (Ablon, Libicki, & Golay, 2014). On the other hand, new war scenarios in the world are making smart cities attractive targets to cyber terrorists. The black market for vulnerabilities in recent years is dominated by more disciplined, organized, and structured groups that often identify specific targets (Ablon et al., 2014). Nations also state that they are already targeting governments for espionage, cyber attacks, and so on. The potential vulnerability of smart cities and e-government to cyber attacks is problematic.

Considering the cyber attack threat on smart cities, one may assume that governments prioritize cybersecurity when building smart cities. The truth is the opposite. Disincentives are common in software development. Smart city technologies are subject to dual disincentives, by both product vendors and city managers, resulting in overall negligence of cybersecurity of smart city products. Some vulnerabilities found in smart products are not a fault of any one device or design choice, but rather a systematic lack of security consciousness (Ghena et al., 2014).

3.2. Vendor's priority

Smart software vendors provide technological products to support smart services. The quality of a smart product has two major aspects, its functionality to provide reliable services and its security to resist against cyber attacks. It is not unusual for software vendors to place functionality over security. Vendors are found with little or no experience in implementing security. Many vendors do not object to giving full privileged access to a device or system to anyone who is on a local network (Cerrudo, 2015). Vendors are averse to making security investments against events that have never occurred, even if they might worry about them. Rather than managing risk, they are closing known vulnerabilities (Dynes, Goetz, & Freeman, 2008).

It is inherent to software development nature that vendors are motivated to prioritize functionality over security. There are two types of vulnerabilities, functional vulnerability from the weaknesses in software products' functionality such as data processing and management vulnerability from the improper management of the codes or the security features (Huang et al., 2015). Most vulnerabilities are functional in early stages of product development. Management vulnerabilities then start to appear, and eventually become the mainstream. It follows that functionality is the prior concern than security in early stages of new product development. As the dominant type of vulnerabilities transfers from the functional to the management as the products mature, vendors are supposed to shift to the security features of their products such as permissions, privileges, and access control.

Vendors face little security demand from buyers. Most users look for solutions that provide maximum functionality. This is not necessarily a bad thing, provided that the technology is safe. Nevertheless, when users buy technology with limited security requirements and without requiring any security testing, this opens the door for vulnerable and insecure technologies to prevail the market. Economic principle suggests that the price the smart product vendor may charge the city on the product depends on how much the city values the product based on its functionality and security features, which in turn determines how much the vendor is willing to invest in product functionality and security. If the city had no concern over security or did not test on security, the price of the product would be merely determined by its functionality.

The vendor lacks also incentives to monitor closely smart city systems after installation. When a system is compromised, the vendor is normally not held financially liable for users' losses (Scott, 2008). The missing obligation of the vendor means that the risk of vulnerability exploitation is taken by the city and its citizens, not by the vendor. Different from vulnerabilities that threat vendors directly, vendors have limited incentives to dedicate resources to find vulnerabilities or purchase vulnerabilities found in their technologies if the attack would not cause much direct financial loss to them other than burdens to patch.

3.3. City government's disincentives

City government's lack of security conscientiousness further disincentivizes vendors to invest in security. In a smart city environment, weak services could cause large scale damage, even affecting social stability and security. Responsible city managers shall implement the best technological solutions with a lower risk and exposure to cyber threats. They ought to test and monitor the security level of smart city products both during and after the process of acquiring new smart technologies. Nevertheless, politicians' goal can be political success rather than social well-being. They are often criticized as making myopic decisions such as the accumulation of government debt (Eslava, 2011) and under-investment in areas with long-term returns like basic research and environmental protection (Margolis & Kammen, 1999). Researchers have long been intrigued by the idea that elections may induce a short-term bias (Nordhaus, 1975).

City managers' myopia may arise from the desire to improve performance of current term while neglecting the potential costs of future outcomes in order to win reelection. Normally, politicians receiving the largest number of votes win elections. Building smart cities can affect the votes in two ways. On the one hand, smart city products improve the quality of life that benefits citizens, which will gain votes. On the other hand, exploitation of smart city vulnerabilities would harm citizens and lose votes, had exploitation occurred.

City managers' lack of security consciousness is a combination of the nature of political accountability and the uncertain and contingent nature of vulnerability exploitation. Political accountability often acts in a post hoc, retrospective manner. Who would be held accountable for the failure of the smart city system when it happened under a different city administration from the one that adopted the system? With the lagging nature of political accountability, the metrics of success and the accountability for failure are diffuse. Elected officials are in for their terms of service. Considering the uncertainty of vulnerability exploitation of smart cities, government leaders serving only for certain terms may not be concerned with future security. Thus, city managers have strong incentives to build smart cities, which helps build service records during the present term and increases the chance of winning reelection, with little concerns of potential cyber security threat on cities.

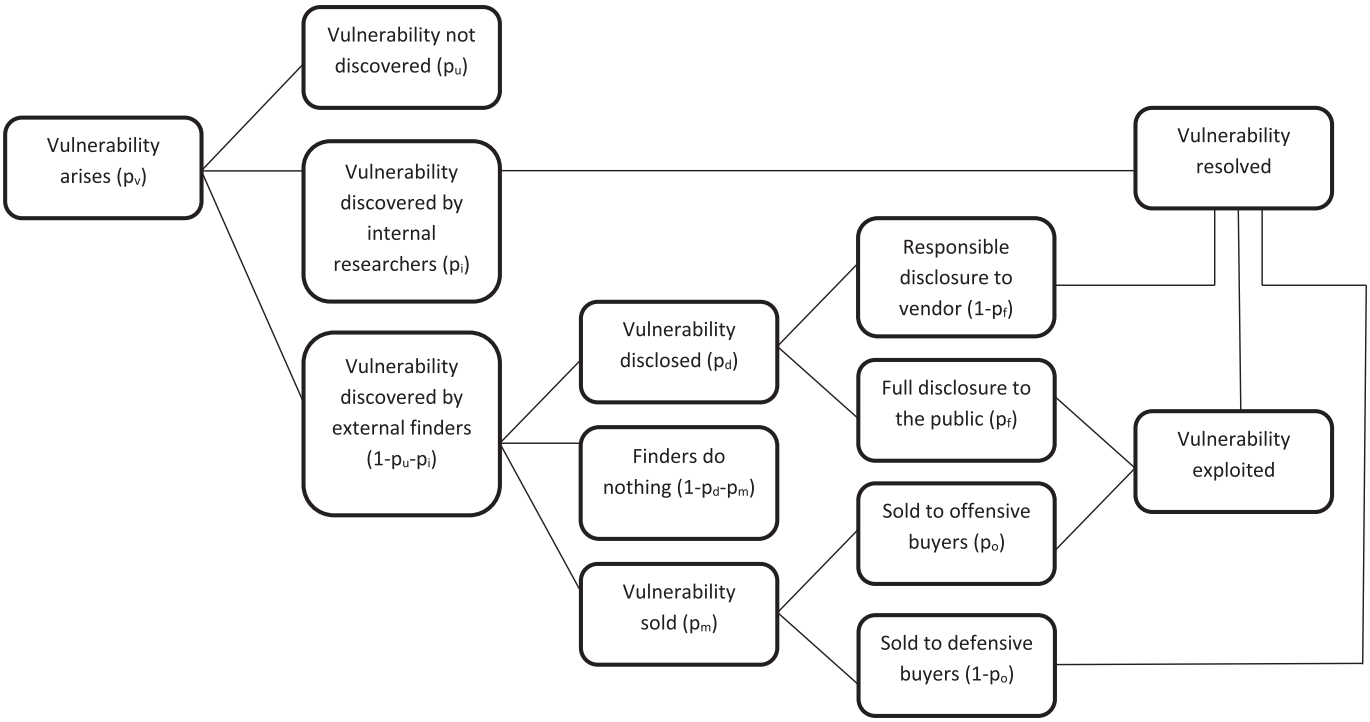


Fig. 1. Phases during the life cycle of vulnerability and the causal relationship of events.

In practice, cities are implementing smart technologies without first testing cybersecurity although they usually rigorously test devices and systems for functionality, resistance to weather conditions, and so on. This is happening around the world (Cerrudo, 2015).

4. The model of smart city vulnerability

The discovery and disclosure of vulnerabilities are processes that are significantly impacted by the economics involved (Anderson & Moore, 2006). To seek for economic solutions to improve cybersecurity of smart cities, we need to understand the economic incentives of various stakeholders in the smart city vulnerability game. In this section, we build a life cycle model of vulnerability that illustrates the relationship between major vulnerability-related events, which leads to further discussion of incentives.

4.1. The life cycle of vulnerability

The life cycle of a vulnerability can be divided into phases between distinct events (Frei, 2013, December). Fig. 1 is a life cycle model tailored to smart city vulnerabilities. Four major phases are included:

- Vulnerability arises: a smart city product with potential vulnerability is released.
- Vulnerability discovered: the vulnerability may be discovered by internal researchers or external vulnerability finders.
- Vulnerability exploited: the vulnerability is disclosed or sold to offensive buyers, resulting in exploitation activities.
- Vulnerability resolved: once the vendor is aware of the vulnerability, it will be able to assess the risk and to resolve the vulnerability. This will occur if the vulnerability is found by internal researchers, if the external vulnerability finder discloses to the vendor, if the vulnerability is purchased by defensive buyers, or if the identified exploitation provides vulnerability information to the vendor.

In the parentheses of Fig. 1 are the probabilities for each event to occur. For example, p_v is the probability that a security vulnerability arises in a smart city product.

Internal researchers are those vulnerability finders affiliated with an organization who will follow proper disclosure policies and procedures to release the vulnerability information to the vendor. External vulnerability finders are freelance researchers who are free to dispose their vulnerability findings. A large percentage of vulnerabilities are found by external finders (Algarni & Malaiya, 2014).

After a vulnerability is discovered by an external vulnerability finder, he/she has several options:

- Do nothing.
- Provide full disclosure of vulnerability information to all affected parties, including potential attackers.
- Privately disclose the finding to the product vendor or to a vulnerability program coordinator before disclosing detailed information to the public.
- Sell the information.

Those who find vulnerabilities and those who exploit them are assumed to be separate groups as attackers largely do not find vulnerabilities independently. Finding vulnerabilities is not an illegal activity, whereas exploiting vulnerabilities generally is. External vulnerability finders represent a critical source of security risk, should they choose to disclose the vulnerability information to the public, or sell the information to malicious vulnerability exploiters.

4.2. The probability of attack

Money and reputation are often the top two concerns for external vulnerability finders when they consider the disposal of their findings.

Reputation and credit help motivate external finders to choose the vendor over attacker. Finders may seek to preserve the right to their claim of findings (Joh & Malaiya, 2009). For those who desire recognition more than money, they may choose to disclose vulnerabilities. The option is between reporting the finding to the vendor or posting the information publicly. Both are for free so which type of

disclosure a finder would choose is more of ethical concerns. It has been found that the majority of vulnerabilities are exploited shortly after they are made publicly known (Brumfield, 2015), hence the probability of exploitation after full disclosure is high.

We assume that full disclosure will for sure lead to vulnerability exploitation so that in Fig. 1, exploitation occurs in case of full disclosure or in case of vulnerability sold to offensive buyers. The total probability of vulnerability exploitation is given by

$$p_v \times (1 - p_u - p_i) \times \{p_d \times p_f + p_m \times p_o\} \quad (1)$$

Before the vulnerability market matured, it was not unusual for finders to pass the vulnerability to the vendor. In recent years more external finders have turned to the vulnerability market to sell their findings (Algarni & Malaiya, 2014). In the life cycle model, this is translated into a rather low value of p_d and a high value of p_m. It is reasonable to presume that external vulnerability finders are largely money driven nowadays, hence $p_d \to 0$ and $p_m \to 1$. Eq. (1) is thus simplified to

$$p_v \times (1 - p_u - p_i) \times p_o \quad (2)$$

Proposition 1. *Events and forces that lead to a smaller probability for a vulnerability to arise, a greater probability for the vulnerability to stay undiscovered or be discovered by internal researchers, or a smaller probability for the vulnerability to be disclosed to attackers will lower the probability of attack.*

Of the four probabilities affecting the probability of attack, the probability for vulnerability to arise in a smart city product (p_v) and the probability the vulnerability is not discovered (p_u) depend on inherent security feature of the product, directly related to the vendor's investment in security during product development process. The probability the vulnerability is discovered by internal researchers (p_i) depends on the vendor's follow-up investment in security researchers after a product is released. They are all related to the vendor's security investment strategy in product design and maintenance, in response to possible financial incentives generated by the government. The probability the vulnerability is sold to offensive buyers (p_o) is a control variable for the vulnerability finder, but it can be affected by the vendor's and the government's strategies in the marketplace. The more are defensive buyers willing to pay, the more likely it is for the finder to sell to defensive buyers, thus less likely to sell to offensive buyers. That is, p_o depends on vulnerability reward programs of the vendor, whether they exist and how the rewards are designed. It may also be influenced by the way the government participates in the vulnerability market.

In the following, we build a game theoretical framework to look at the interactions among the government, the product vendor, the external finder of vulnerabilities and the attacker with a focus on how financial mechanisms can be created to change game outcomes.

4.3. Game theoretical analysis

In our game setup, we consider four economic agents involved in the life cycle of a smart city vulnerability: the software vendor that produces and sells smart city products, the external vulnerability finder who discovers the vulnerability in the product, the malicious attacker who exploits the vulnerability to hack smart cities, and the government. The government in this context may include government agencies at any level, federal, state, and local, with the goal of achieving cybersecurity of smart cities. By studying the interactions among these players, we consider how the government's strategies affect the vendor's security investment decision, the vulnerability finder's decision on the disposal of the vulnerability, and the expected payoff of the attacker.

In an ideal situation, the external finder shall seek no reward and submit the vulnerability via a responsible disclosure mechanism. This would be the case for those finders for whom getting recognition is sufficient compensation. Nevertheless, this is not enough for many finders since vulnerabilities can have significant economic values. We assume the finder in the game is money driven who desires immediate economic payoffs. Although the fame received from responsible disclosure may eventually translate into economic opportunities, it is not as attractive as present financial gains, i.e., $p_d = 0$. This is equivalent to a single stage game setting which eliminates also the finder's incentive to hold onto the discovery in seek of higher expected returns in future stages. Thus, the money-driven finder will choose to sell the vulnerability for sure, i.e., $p_m = 1$. The probability of vulnerability exploitation is hence as given in Eq. (2).

The expected payoff from vulnerability exploitation to the attacker is

$$\{p_v \times (1 - p_u - p_i) \times p_o\} \times V \quad (3)$$

Given the value of exploitation to the attacker (denoted by V), the expected payoff to the attacker decreases as the exploitation probability decreases. To effectively defend smart cities and e-government against cyber attacks, economic solutions have to focus on reducing this probability because V is largely composed of noneconomic (e.g., political, military) factors in case of hacking smart cities. Economic mechanisms can be designed to motivate the vendor to invest in security and to encourage market participation by defensive buyers.

5. Economic solutions to improve smart city cybersecurity

In this section, we analyze two economic methods that can be used to reduce the chance of cyber attacks on the smart city: creating incentive mechanisms to motivate the vendor to improve product security (to lower p_v, and raise p_u and p_i); using the vulnerability market for defensive buyers to acquire the vulnerability from the external finder (to lower p_o).

5.1. Correcting vendor's disincentives

The more information technologies are involved in the creation and operation of the smart city, the greater the potential risk of cyber attacks. If the cybersecurity issues of smart city products were not addressed early on, the cost and complexity of creating a smart city could make it far more difficult to address down the road. In the end, the city would be left vulnerable. It is essential to the cybersecurity of the city to correct the disincentives of smart city product vendors to motivate them to provide safe products and technologies.

Consider functionality and security of a smart city product. Let P be the price of the product. If the city values both functionality and security, then the price of the product depends on both of the product features, i.e., $P = P(f,s)$, where f measures the level of functionality, and s measures the level of security. The cost structure of the vendor depends on its investment in functionality and security of the product, denoted by $C = C(f,s)$. The total cost is increasing in the level of functionality and security of the product.

If the vendor does not gain from increased security (by selling products at a higher price), or does not suffer from a product failure (facing no financial punishment), the profit-maximizing strategy for the vendor is to minimize expenditure on security (i.e., $s = 0$). The vendor's profit from supplying the smart city product to the city is $\pi = P(f) - C(f)$.

When security does not appear in the profit function of the vendor, to maximize profit, the vendor chooses the optimal level of functionality f^* that satisfies $P'(f) = C'(f)$. The maximum profit gained by the vendor is

$$\pi^*_{s=0} = P(f^*) - C(f^*) \quad (4)$$

To correct for the lack of security concern by the vendor, either value of security has to be attached to the price of the product or the vendor must be held financially responsible for loss from product failure. The former requires the government to be willing to pay not

only for functionality of a product, but also its security. The latter requires some punishment mechanism to force the vendor to be at stake when an attack occurs.

5.1.1. Rewarding vendor for security enhancement

One way to provide financial incentives for the vendor to invest in security is to reward the vendor for improved security.

When security enters both the revenue and the cost side of the vendor's choice, the profit function becomes $\pi = P(f,s) - C(f,s)$. The vendor now has two decision variables, functionality and security. The vendor chooses the optimal strategy $\{f^*, s^*\}$ that satisfies $P_f(f,s) = C_f(f,s)$ and $P_s(f,s) = C_s(f,s)$. The optimal profit accordingly is

$$\pi^*_{s=s^*} = P(f^*, s^*) - C(f^*, s^*) \tag{5}$$

Proposition 2. *Given the city's desired security level s^d, there exists a security premium so that $s^* = s^d$.*

Proof. Given the cost structure of the vendor, it is the security premium (the increase in product price due to enhanced security) the city is willing to pay that determines the vendor's willingness to invest in security. As long as $\pi^*_{s=s^*} > \pi^*_{s=0}$, the vendor would choose to invest in security to reach the optimal level $s^* > 0$. As the security premium increases, product security increases. The city can induce the desired level of security from the vendor by offering a security premium payment at which $P_s(f^*,s^d) = C_s(f^*,s^d)$. Q.E.D.

A couple of prerequisites for this solution to work:

- The city needs to test on security (not merely functionality) of the product to determine its security level.
- The pricing function needs to be linked to security.

The challenge of this approach lies in the difficulty of measuring security (Pfleeger & Cunningham, 2010), thus it may not be easy to effectively place a premium on securer software. Nevertheless, what is actually required on the city side is to signal vendors that they will be rewarded for security. Once this becomes a general practice, the supply-and-demand forces in the market for smart city products will set the equilibrium security premium function for calculating total security premium at various levels of security.

5.1.2. Punishing vendor for vulnerability exploitation

No product is perfectly secure. There is always a chance for the product to be hacked even if $C(s) = \infty$. Suppose the product is hacked in the tth year from its release that causes a loss of M_t, the present value of the loss is $\frac{M_t}{(1+i)^t}$, where i is the discount rate, such as applicable market interest rate, used to convert a future loss to the present (the installation date of the product), and $\frac{1}{(1+i)^t}$ is the discount factor. The expected loss of exploitation valued in today's dollar (denoted by L) is the weighted average of present values of the exploitation losses that occurred during the lifespan of the product (n years). The weights are the discount factors, i.e.,

$$L(s, M) = \sum_{t=0}^{n} \{p_v \times (1 - p_u - p_i) \times p_o\} \times \frac{M_t}{(1+i)^t} \tag{6}$$

where $\{p_v \times (1 - p_u - p_i) \times p_o\} \times \frac{M_t}{(1+i)^t}$ is the present value of the expected loss of exploitation occurred t years from the installation of the product. For simplicity, the probability of attack is held constant over time.

The expected loss depends on the probability of vulnerability exploitation and the actual loss occurred. It is decreasing in exploitation probability and increasing in the size of loss, i.e., $L_s(s,M) < 0$ and $L_M(s,M) > 0$. If the loss to the city were to be covered by the vendor, this would be contingent cost to the vendor in addition to its existing cost of production.

At the presence of the contingent financial punishment, the objective function of the vendor becomes

$$\pi = P(f) - C(f, s) - L(s, M) \tag{7}$$

The M component of the contingent cost function is assumed exogenous to the vendor. What the vendor controls is the level of security that affects the likelihood of vulnerability exploitation.

Proposition 3. *Given the city's desired security level s^d, there exists a financial liability L(s,M) in the range of $[0, \pi^*_{s=0}]$ so that $s = s^d$.*

Proof. The profit-maximizing security level solving the first-order condition of Eq. (7) satisfies

$$C_s(f, s) + L_s(s, M) = 0 \tag{8}$$

The maximized profit can be positive and negative. Considering the significant damage cyber attacks may impose on the city, the maximized profit is highly likely to be negative. Since the vendor would not be willing to supply a product with expected loss, the actual financial liability of the vendor cannot exceed $\pi^*_{s=0}$. Normally, security investment cost is less than the attack loss of the city. The financial liability constraint is not bound so that the city may induce the desired level of security by choosing the financial liability of the vendor $L(s,M)$ in the range of $[0, \pi^*_{s=0}]$ at which the vendor's choice of security satisfies Eq. (8). Q.E.D.

There can be variations of the financial punishment mechanism, such as to attach a termination date, equivalent to the term of warranty. Practice can be of different ways. What is essential is to have the vendor share vulnerability risks with the city without eliminating the vendor's incentive to supply the smart city product. The proposed punishment mechanism has more signaling effect to motivate the vendor to invest in security ex ante rather than to punish the vendor ex post.

Indeed, such contingent financial punishment may motivate the vendor to create a bug bounty program. The vendor's willingness to pay to the vulnerability finder depends on the expected penalty. The vendor will be better off if the vulnerability reward paid to the finder is less than the expected penalty. The maximum possible reward the vendor is willing to pay is also capped by $\pi^*_{s=0}$. It is not easy to gauge the financial liability of the vendor for the loss of the city. The bottom line is the vendor has to be held at least partially financially responsible for the loss. The vendor also needs to pay the patching cost of found vulnerabilities. It has been found that vendor liability for patching costs can be more effective than vendor liability for damages (August & Tunca, 2011).

5.2. Acquiring vulnerability in the market

Government and vendor can actively participate in the vulnerability market to prevent the vulnerability from being obtained by malicious attackers.

5.2.1. The market for vulnerabilities

Vulnerabilities are holes in computer systems that can be exploited to infiltrate malware, spyware or allow unwanted access to user information. Software vulnerabilities can be traded in the market place (Miller, 2007).

The current vulnerability market consists of three categories: the white market where vulnerabilities are sold to software vendors or other companies that work with the vendors to rectify security flaws; the black market where vulnerabilities are sold to exploiters; and the intermediate gray market (Stockton & Golabek-Goldman, 2013).

The white market is regulated where the transactions are properly documented and disclosed. Vulnerability reward programs by vendors are a major part of the white market. There are also third-party security organizations such as iDefense's Vulnerability Contributor Program (VCP) and HP Tipping Point's Zero Day Initiative (ZDI) that buy vulnerabilities and sell to software vendors.

The black market is not regulated by any laws, and market

transactions are not recorded. It has no attempt to safeguard the society, and allows any buyer such as cyber criminals and terrorists to buy vulnerabilities. The price paid is said to be five to ten times higher than other vulnerability markets (Algarni & Malaiya, 2014).

On the gray market, vulnerability and exploit brokers like Vupen and ReVuln buy and sell vulnerabilities, provide a link between a vulnerability finder and a buyer, and gain revenue from charging commission of the selling price. They may sell vulnerabilities to the vendor or some government organization, depending on who is willing to pay more. They advertise that they sell knowledge of vulnerabilities for cyber espionage and in some cases for cyberweapons. Government agencies in several countries have become major players in the gray market. Transactions on the gray market can be termed legitimate or improper, depending on the point of view.

5.2.2. The use of vulnerability market

The vulnerability finder seeking to sell the vulnerability discovery may share it with responsible disclosure programs and get the reward, sell on the black market but facing potential criminal prosecution, or arrange a deal through an exploit broker. Ultimate buyers of the exploit information can be defensive or offensive. Defensive buyers intend to defend the product against cyber attack. They will use the purchased vulnerability information to patch the product and make it securer. Offensive buyers intend to use the vulnerability to exploit.

Of the four parties in the vulnerability game, the external finder is on the supply side of the vulnerability market. The other three - government and vendor as defensive buyers, and attacker as offensive buyer - are all on the demand side. The finder has the power to choose to whom to sell, while the demand side is highly competitive. If the finder sold for price difference only, the vulnerability would go to the buyer who is willing to pay the most.

To improve smart city cybersecurity, we propose active market participation by defensive buyers, especially the government, in order to reduce the chance that vulnerability information is purchased by offensive buyers.

Vendors are already participating in the marketplace as defensive buyers, largely through vulnerability reward programs, but the participation is limited. Currently, there are only a few vulnerability reward programs by vendors, most of which were created a few years ago (Algarni & Malaiya, 2014). There are several reasons why selling vulnerabilities to vendors can be attractive, including the decreased risk of getting ripped off and the possibility of future job offers. Finders receive also recognition. The vulnerability reward programs deserve further development. They were found to be economically efficient, comparing favorably to the cost of hiring full-time security researchers to locate bugs internally (Finifter et al., 2013).

Vendors' reward programs are a good option for finders to sell in an easy and legitimate way, but they do not offer anywhere near the prices offered in the underground market. When a government agency is a buyer, nevertheless, the money it can bring to the table may be unable for other buyers to match. Government can be highly competitive in the market. Its willingness to pay for a smart city vulnerability is capped by the actual loss to the city if the vulnerability is exploited (M). As $\pi^*_{s=0} \ll M$ is normally the case, the government's economic interest in participating the vulnerability market largely exceeds that of the vendor. The government may be able to pay much more to the finder compared to the vendor, thus largely increasing the chance for the vulnerability to fall in the hands of defensive buyers.

Governments around the world are already buying vulnerabilities, normally for offensive purpose. We argue that government agencies with defensive purpose shall also participate in the vulnerability market to compete with malicious buyers. Considering the inequality between the loss to the city and the gain to the hacker, having governments join the buying side of smart city vulnerabilities can be an effective way to prevent attacks on smart cities.

While the vulnerability market has developed, vulnerability commercialization remains a controversial issue. One controversy is about the buyers' intents. The issue could be less controversial if more vulnerabilities were purchased for defensive purpose.

5.2.3. Market dynamics with government being defensive buyer

The active participation in the marketplace by the government as defensive buyer will increase market demand for vulnerabilities. The government's willingness to pay a higher price than other buyers will also increase the price elasticity of demand in the market. In the supply-and-demand model, this leads to a rightward shift in the market demand curve and the curve becomes also flatter. How does this change in demand affect the market? It depends on the responses by the supply side over different time horizons.

In the following, we use the supply-and-demand model to analyze the effects of having the government as defensive buyer in the vulnerability market (Fig. 2). In all the graphical illustrations, point A is the initial market equilibrium and point B is the new market equilibrium with government acting as defensive buyer. Q represents the initial purchase of vulnerabilities by offensive buyers which is also the initial market equilibrium quantity, Q' is the new level of vulnerability purchased by offensive buyers, and Q'' is the new market equilibrium quantity of vulnerabilities.

Case I. The number of vulnerabilities supplied to the market is fixed.

As a starting point, we consider the case in which the market supply curve is vertical. This allows us to study the immediate response in the market when the quantity of available vulnerabilities for sale is unchanged yet. The increase in demand for vulnerabilities generated by the government does not change the number of vulnerability transactions, but it increases the market price of vulnerabilities. The effect is shown in Fig. 2a. The increased price drives a portion of offensive buyers out of the market. The quantity of vulnerabilities sold to offensive buyers decreases from Q to Q', and the government's purchase of vulnerabilities is $(Q'' - Q')$.

Case II. External vulnerability finders respond to price changes.

In this case, the market supply curve has its normal upward sloping shape. We assume that vulnerability finders are purely money driven, thus the increase in market demand for vulnerabilities does not shift the supply curve. The effect is shown in Fig. 2b. What higher demand does to the supply side of the market is to induce more vulnerabilities to be supplied to the market by pushing up the market price of vulnerabilities.

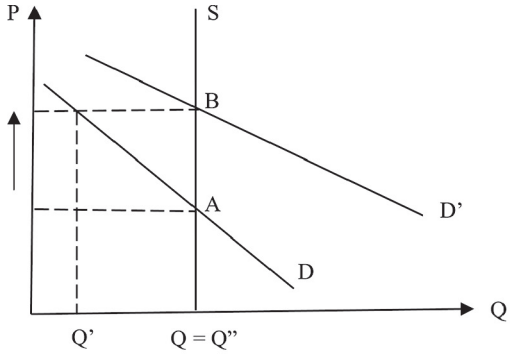
The decrease in the quantity of vulnerabilities purchased by offensive buyers is $(Q - Q')$. The government's purchases of vulnerabilities is $(Q'' - Q')$. That is, although higher demand induces vulnerability finders to supply more vulnerabilities to the market, the increased vulnerabilities are purchased all by the government. Additionally, a fraction of vulnerabilities that would have been purchased by offensive buyers are now purchased by the government as well.

Case III. Vulnerability finders respond to price and non-price factors.

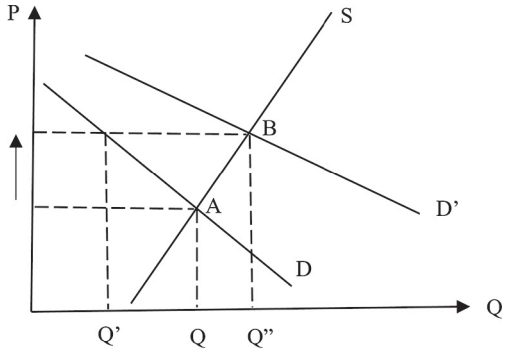
Taking into account non-financial factors such as legal and ethical that can also affect to whom vulnerability finders sell, government presence in the market as defensive buyer provides attractive alternatives for vulnerability finders, which increases their supply of vulnerabilities when selling vulnerabilities becomes less controversial or risky. The effect is shown in Fig. 2c. It is also possible for the supply curve to become flatter when external finders are willing to sell to the government at a lower price compared to selling to attackers. Theoretically when both demand and supply increase in a market, the change in price is ambiguous. Considering incentives and technical restraints, the increase in supply in the vulnerability market is likely to be less than the increase in demand, thus the market price is more likely to rise, as illustrated in the figure.

The above analysis leads to the following proposition.

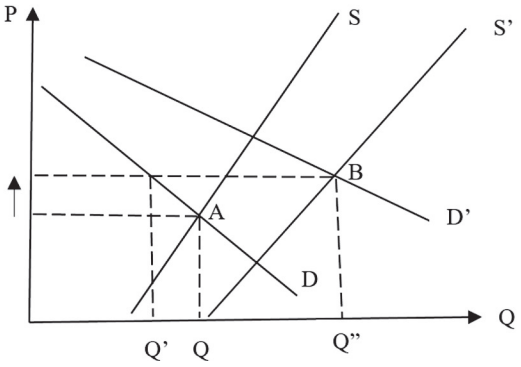
Proposition 4. *If government acts as defensive buyer, the market price of*



(a) Very short run effects when the market supply curve is vertical, i.e., the quantity of vulnerability supplied to the market by external finders is fixed immediately after the government enters the market.



(b) Effects on the market when market supply has its normal upward sloping shape, i.e., external finders respond to monetary incentives created by the government participation in the market.



(c) Effects on the market when market supply increases, i.e., external finders respond to both monetary and non-monetary incentives created by the government participation in the market.

Fig. 2. Responses in the vulnerability market when government acts as defensive buyer.

vulnerability rises, the quantity of vulnerability purchased by offensive buyers decreases. The government's cost of acquiring vulnerabilities is reduced when vulnerability finders respond to both monetary and non-monetary factors.

In all cases, offensive buyers are worse off: they obtain fewer vulnerabilities at higher price. Unless in the very short run (Case I), the quantity of vulnerability traded in the market increases due to government purchases of vulnerabilities. This is not necessarily bad as the government acquires more vulnerability information, and the effective quantity of vulnerabilities bought by attackers decreases, making smart cities and e-government securer.

5.3. Policy instrument design

The security of smart cities is essentially in the hands of the government. Various stakeholders may have their own smartness and security assessment, but the responsibilities, process execution and decision making need to be institutionalized, where the government takes ownership of the arrangement for the safe future of smart cities. In the following, we provide some outlines for the design of cybersecurity policy instruments by the government.

First of all, governments shall take the initiative to build smart cities in a secure way. They shall specify the governmental role in the regulation of publicly accessible solutions by vendors, and the verification of adequate compliance and control over offered smart city services. They may use command-and-control policy to manage the smart city information system. Nevertheless, much like dealing with other social problems, market-based solutions are generally more effective. The life cycle analysis of vulnerabilities and the revenue-cost analysis of product vendors give insights on choosing working economic solutions to motivate non-government stakeholders of smart cities.

Preventive measures and ex-ante investment in security shall have the priority than ex-post cleanup and crisis management. To facilitate the reward and punishment mechanisms to motivate product vendors to supply secure products, governments are expected to establish communication with vendors to specify consensus on the minimum security baseline. Governments verify vendors' claims about the security feature

of their products, and emphasize only highly secured and thoroughly tested products are rolled out. Solutions are audited for security vulnerabilities and compliance with the security baseline. Liability of vendors needs to be clearly defined and measurable. As for motivating governments, one possibility is to have an independent government office that isolates the political aspects from the technological aspects of the government. Another possibility is to hold government liable for adopting insecure technologies.

In reality, most of the cybersecurity resources are coming from federal and state governments. City government buying vulnerabilities from the market is not the standard practice. Local governments may have to depend on information sharing with other government agencies (Welch, Feeney, & Park, 2016). This is especially true for smaller governments that may not have the resources necessary to defend themselves although they still need to provide much the same range of technology services as larger governments.

Policymaking in cybersecurity faces many paradoxes in the current practice. One difficulty lies in the ambiguous and overlapping distribution of responsibilities across many government agencies at various levels. Effective collective actions require clear definition of responsibilities and effective communication tools. There are a variety of ways governments can collaborate. One possibility is to let city government take the lead, and other government agencies provide necessary support to supplement lack of resources at the city level. To reduce the level of exposure to cyber attacks, governments may cooperate to share technology services with one government providing services to several cities.

No resources are free. Government collaboration in information sharing helps reduce cost. Law and enforcement punishing cyber attacks and illegal selling of vulnerability to attackers helps increase vulnerability finders' willingness to sell to the government, which may further reduce cost.

5.4. Limitation and future research

This study provides a theoretical framework of incentive structures policymakers may consider in security policy design. The effective implementation of the proposal has several prerequisites, which is the limitation of this study and is also the direction of future research. Some limitations are technical such as how to measure the security quality of a smart city technology. Most are non-technical, including economic, institutional and legal challenges.

Economically, the challenges are mainly with vulnerability valuation and government budget management. The proposed economic alternatives to motivate the vendor to invest in security and to encourage defensive buyers to participate in the vulnerability market require further study on the working formula to link payment to security, to link breach cost to shared responsibilities between the government and the vendor, and the cost-benefit analysis of cybersecurity defense and government spending.

Government collaboration is essential for effective government participation in the marketplace. Local governments face various policy and political constraints to play an essential role in the market. Upper-level governments, especially federal agencies, have been participating in the marketplace but largely for offensive purpose. Existing government actions can be strengthened and used for defensive purpose as well. Future research can be carried out regarding institutional and legal issues associated with governments' vulnerability market participation and how to create collaboration mechanisms to pool government cybersecurity resources and avoid unnecessary competition among government agencies in the marketplace. Further research can also be done in dynamic interactions among stakeholders, and various policy instruments that can be implemented.

A formal test of model predictions and policy recommendations goes beyond the scope of this study. It will be worthwhile to further develop the topic with empirical analysis. Smart city cybersecurity is a practical issue. Case studies are necessary to learn various government experiments in introducing incentive mechanisms and marketplace experiences.

6. Conclusion

Along with the fast development of smart city technologies is the increasing cybersecurity threat on smart cities and e-government. What is essential to the success of smart city efforts is the reliability and security of smart city products. Compared to the functionality feature of these products, their security quality is often neglected. The security level of a smart city technology is not merely the decision-making by the product vendor, it is the result of interactions among multiple stakeholders with conflicting or compatible interests. The strategy of one party can affect the choices of others. Government policies are government decisions creating incentives and disincentives. What economic incentives the government may create to improve smart city cybersecurity is the major issue we were interested to address in this study.

In particular, we aimed to explore working economic solutions to make smart cities securer. Intuitively, any technological products would be securer if they are produced with higher level of security, or found vulnerabilities are patched by vendors before the information is exploited by attackers. By modeling the life cycle of vulnerabilities, we identified the key factors determining the probability of cyber attacks. Based on the analysis of the probability and incentives, we proposed two alternative economic solutions the government may use to address the cybersecurity challenges facing smart cities and e-government, including the creation of incentive mechanisms for vendors to invest in security, and the usage of the vulnerability market for defensive buyers to acquire vulnerabilities to prevent the vulnerability information from falling into the wrong hand.

The key difference between the two proposals is the split of financial responsibility between the government and the vendor. In cases of rewarding the vendor for improved security and having the government purchase the vulnerability, the government picks up the tab; in cases of punishing the vendor for vulnerability exploitation and having the vendor pay for vulnerability, the vendor pays the bill. Nevertheless, economic theories tell us that essentially, the vendor (as the seller of the product) and the government (as the buyer of the product) will share the financial burden of vulnerability. In which way the burden is shared depends on market forces of supply and demand of smart city products.

Vulnerability market is growing fast in the new digital era. Vulnerability finders today largely choose vulnerability disclosure in the marketplace. Governments have been participating in the market for defensive purpose such as espionage and cyber warfare. The disclosure of vulnerabilities to malicious attackers can be significantly reduced with increased market participation by government as defensive buyer. Given the unbalanced distribution of limited defense resources, collaboration and coordination of various government agencies are important considering budget constraints and practical feasibility.

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. *Rand corporation research report.*.

Algarni, A. M., & Malaiya, Y. K. (2014). Software vulnerability markets: Discoverers and buyers. *International Journal of Computer, Information Science and Engineering, 8*, 71–81.

Alsultanny, Y. A. (2014, September–October). Evaluating users intention to use e-government services. *International Journal of Emerging Trends & Technology in Computer Science, 3*, 55–60.

Anderson, R., & Moore, T. (2006). The economics of information security: A survey and open questions. *Science, 314*, 610–613.

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure: An empirical analysis. *Information Systems Frontiers, 8*, 350–362.

Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science, 54*, 642–656.

August, T., & Tunca, T. I. (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science, 57*, 934–959.
Belanche-Gracia, D., Casalo-Arinob, L. V., & Perez-Rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Government Information Quarterly, 32*, 154–163.
Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM conference on computer and communications security* (pp. 833–844). Raleigh, NC.
Brumfield, J. (2015). *Verizon 2015 data breach investigations report*.
Cerrudo, C. (2015). *An emerging US (and world) threat: Cities wide open to cyber attacks*. IOActive White Paper.
Cocchia, A. (2014). Smart and digital city: A systematic literature review. In R. P. Dameri, & C. Sabroux (Eds.). *Smart city: How to create public and economic value with high technology in urban space* (pp. 13–43). Switzerland: Spri nger International Publishing.
de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*, 1–7.
Dynes, S., Goetz, E., & Freeman, M. (2008). Cyber security: Are economic incentives adequate? *IFIP International Federation for Information Processing, 253*, 15–27.
Eslava, M. (2011). The political economy of fiscal deficits: A survey. *Journal of Economic Surveys, 25*, 645–673.
Finifter, M., Akhawe, D., & Wagner, D. (2013). An empirical study of vulnerability reward programs. *Proceedings of the 22nd USENIX conference on security* (pp. 273–288). Washington, D.C.
Frei, S. (2013, December). *The known unknowns: Empirical analysis of publicly unknown security vulnerabilities*. NSS Labs.
Frei, S., & Artes, F. (2013, December). *International vulnerability purchase program: Why buying all vulnerabilities above black market prices is economically sound.* NSS Labs.
Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. *Woot'14 proceedings of the 8th USENIX conference on offensive technologies* (pp. 7-7). San Diego, CA.
Herr, T. (2017). Governing proliferation in cybersecurity. *Global Summitry, 3*.
Huang, K., Zhang, J., Tan, W., & Feng, Z. (2015). An empirical analysis of contemporary android mobile vulnerability market. *Proceedings of the 2015 IEEE international conference on mobile services (ms)* (pp. 182–189). New York, NY.
Illera, A. G., & Vidal, J. V. (2014). *Lights off! The darkness of the smart meters*. The Netherlands: Black-hat Europe Amsterdam RAI.
Joh, H., & Malaiya, Y. (2009). Seasonal variation in the vulnerability discovery process. *Proceedings of ICST '09, international conference on software testing verification and validation* (pp. 191–200). Denver, CO.
Kitchin, R. (2016). Reframing, reimagining and remaking smart cities. *The programmable city working paper 20.*.
Klaper, D., & Hovy, E. (2014). A taxonomy and a knowledge portal for cybersecurity. *Proceedings of the 15th annual international conference on digital government research* (pp. 79–85). .
Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber-risk and cyber-security. *Government Information Quarterly, 33*, 250–257.
Li, Z., & Liao, Q. (2016). An economic alternative to improve cybersecurity of e-government and smart cities. *Proceedings of the 17th international digital government research conference on digital government research* (pp. 455–464). Shanghai, China.
Margolis, R. M., & Kammen, D. M. (1999). Evidence of under-investment in energy R & D in the United States and the impact of federal policy. *Energy Policy, 27*, 575–584.
Mein, A., & Evans, C. (2011, March). *Dosh4Vulns: Google's vulnerability reward programs*.
Miller, C. (2007). The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. *Proceedings of the sixth workshop on the economics of information security.* Pittsburgh, PA.
Mojica, I. J., Adams, B., Nagappan, M., Dienst, S., Berger, T., & Hassan, A. E. (2014). A large-scale empirical study on software reuse in mobile apps. *IEEE Software, 31*, 78–86.
Nordhaus, W. D. (1975). The political business cycle. *Review of Economic Studies, 42*, 169–190.
Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*, 245–253.
Pfeiffer, M. H. (2015). *Managing technology risks through technological proficiency: Guidance for local governments*. Bloustein Local Government Research Center, Rutgers.
Pfleeger, S., & Cunningham, R. (2010). Why measuring security is hard. *IEEE Security & Privacy, 8*, 46–54.
Quigley, K., Burns, C., & Stallard, K. (2015). 'cyber gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly, 32*, 108–117.
Ransbotham, S., Mitra, S., & Ramsey, J. (2012, March). Are markets for vulnerabilities effective? *MIS Quarterly, 36*, 43–64.
Sa, F., Rochac, A., & Cota, M. P. (2016). Potential dimensions for a local e-government services quality model. *Telematics and Informatics, 33*, 270–276.
Scott, M. D. (2008). Tort liability for vendors of insecure software: Has the time finally come? *Maryland Law Review, 67*, 425–484.
Stockton, P. N., & Golabek-Goldman, M. (2013). Curbing the market for cyber weapons. *Yale Law & Policy Review, 32*, 101–128.
Sureshchandra, S. M., Bhavsar, J. J., & Pitroda, J. R. (2016). Review on identification of success factors for designing of smart cities. *International Journal of Science Technology & Engineering, 2*, 125–133.
Welch, E. W., Feeney, M. K., & Park, C. H. (2016). Determinants of data sharing in U.S. city governments. *Government Information Quarterly, 33*, 393–403.
Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. *Government Information Quarterly, 31*, 150–159.
Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*, 49–56.

Dr. Zhen Li is an E.Maynard Aris Endowed Professor of Economics in the Department of Economics and Management at Albion College, USA. She holds a master's degree and PhD in Economics from Princeton University, USA. She graduated with her bachelor's degree in International Economics from Peking University, China. Dr. Li's recent research interests include inter-disciplinary research study in economics and game theory of computer networks and information security.

Dr. Qi Liao is an Associate Professor of Computer Science at Central Michigan University, USA. He received his MS and PhD in Computer Science and Engineering from the University of Notre Dame, USA. He graduated summa cum laude with a B.S. and Departmental Distinction in Computer Science with a minor concentration in Mathematics from Hartwick College, USA. His research interests include computer security, visual analytics, and economics/game theory at the intersection of network usage and cybersecurity. Dr. Liao's research has been recognized by USENIX and IEEE best papers, Emerald Literati Awards, national competitions, and other academic awards. Dr. Liao was a visiting scientist at IBM Research and an ASEE Fellow for United States Air Force Research Laboratory.