# Solutions and Challenges to Promoting Strong Public Cybersecurity Practices

Daniel Kochik and Wesley Pendergist

American University, School of Public Affairs

Master of Public Administration Capstone

Professor Jocelyn Johnston

April 2017

# Table of Contents

# Abstract

Data privacy and protection of user information is fundamental to the interests of individuals and both public and private institutions. The Ponemon Institute, LLC, on behalf of McAfee, Inc. estimated that data breaches cost the global economy around $445 billion globally. [1] Other estimates suggest that malicious cyber activity may cost the American economy up to $120 billion annually.[2] Public and private organizations benefit from sound cybersecurity practices, and while most institutions follow a set of principles, efforts to reduce instances of breaches are diminished due to the poor practices of general users of commercially available software products, such as Microsoft Windows. We assert that this represents one among several market failures in the cybersecurity market, and some aspects of cybersecurity are a public good that require government regulation to protect the data privacy rights of individuals. We interviewed three cybersecurity experts in public organizations to determine the existing regulatory framework, identify weaknesses, and investigate the potential legal and administrative challenges of implementing policies to promote safer cybersecurity practices.

# 1.0 Introduction/Thesis/Research Questions

Recent technological advances have allowed for unparalleled levels of connectivity and communication. The phenomena, frequently referred to as the "internet of things," has allowed for a massive network of user devices that have the ability to control many aspects of modern life, including smartphones, modern automobiles, and home appliances. The increasing number

[1]" Net Losses: Estimating the Global Cost of Cybercrime Economic: Impact of Cybercrime II". *Center for Strategic and International Studies* on behalf of McAfee, Inc. June 2014. https://goo.gl/RRZ36N

[2] "The Economic Impact of Cybercrime and Cyber Espionage". *Center for Strategic and International Studies* on behalf of McAfee, Inc. July 2013. https://goo.gl/2UIsI0

of devices and their users, however, has broad reaching effects on data privacy rights, the economy, and national security.

Data breaches in the United States, alone, have affected nearly every major industry. A 2015 data breach of the Office of Personnel Management affected the personal information, including the social security numbers, of over 20 million federal employees and applicants.[3] The 2016 data breach at Yahoo was the largest in history, with the breach of nearly 500 million user accounts.[4]

The cost of data breaches for organizations has increased steadily over the last several years, and the average total cost of a data breach for companies about $7.01 million in 2016. [5] From an industry perspective, public organizations fare better than other industries in terms of costs as a result of data breaches, with a $86 loss for per compromised record in 2016, versus $402 per record for the health industry.[6] Yet the implications of such breaches require organizations to take steps to introduce protocols that are designed to protect networks and privacy. President Barack Obama signed Executive Order 13636 in 2013 entitled, "Improving Critical Infrastructure Cybersecurity", to integrate cybersecurity practices into the procurement process.[7] This prompted the National Institute of Standards and Technology's "Cybersecurity Framework of 2014", which sets forth industry standards for businesses and organizations for

[3] Olorunnipa, Toluse and Chris Strohm. "Hackers Stole U.S. Data on More Than 20 Million People". *Bloomberg.* July 5, 2015. https://goo.gl/fv4QfP

[4] Ford Matt. "Yahoo's Half-Billion Hack". *The Atlantic.* Sept. 22, 2016. https://goo.gl/iEaBwC

[5] "2016 Cost of Data Breach Study: United States". *Ponemon Institute LLC, on behalf of IBM.* June 2016. Pg. 2. https://goo.gl/kzk8yu

[6] *Ibid.* Pg. 7.

[7] "Executive Order: Improving Critical Infrastructure Cybersecurity". *The White House, Office of the Press Secretary.* Feb. 12, 2013. https://goo.gl/nO8wU9

managing cybersecurity risks for critical industry.[8] The guidelines were developed in cooperation with the public and private sectors and provide five core functions including the identification of risks, protection, detection of occurrences, and response to detected events.[9] Additionally, the framework provides implementation guidance for industry.[10] In January 2017, the agency issued a revised Draft Version 1.1 of the framework.[11]

The Federal Information Security Modernization Act (FISMA) of 2014, which was passed under Senate Bill 2521 in December 2014, amended federal regulations under 44 CFR 35 to "...provide comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets".[12] The Act provides requirements and responsibilities for federal agencies and requires yearly independent evaluation of agency programs and practices. Moreover, the Act provides for additional coordination between agencies to protect federal information and information systems. In addition, the Act provides that individual agencies are responsible for procuring technical hardware and software information security solutions.[13]

In March 2017, the Office of Management and Budget released its annual report to Congress regarding the state of federal cybersecurity under FISMA requirements for Fiscal Year 2016.[14] The report indicated that there were 30,899 cyber incidents that affected federal agencies

[8] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0". *National Institute of Standards and Technology*. Feb. 14, 2014. https://goo.gl/TyBlP5

[9] *Ibid*. Pg. 8.

[10] *Ibid.* Pg. 12.

[11] Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1". National Institute of Standards
and Technology. Jan. 10, 2017. https://goo.gl/5cgeBm

[12]"S.2531- Federal Information Security Modernization Act of 2014." 113th Congress (2013-2014). https://goo.gl/jd7YbQ

[13] *Ibid*.

[14]"Federal Information Security Modernization Act of 2014: Annual Report to Congress - Fiscal Year 2016". The Office of Management and Budget. March 10, 2017. https://goo.gl/Rjp69S

during 2016, with loss or theft of equipment as the single largest incident and attacks executed from websites or web-based application as the second largest incident type.[15] The report also assessed agency performance and found that several more agencies had improved their anti-phishing, malware, and other defenses over the previous year.[16]

President Donald Trump has signaled that cybersecurity will be a focus of his administration, with an initial budgetary request of $1.5 billion for program expenditures for the Department of Homeland Security for Fiscal Year 2018 to protect federal networks and critical infrastructure.[17] Yet the public remains relatively skeptical about the government's efforts to protect individual data as indicated by a 2014 Pew Research Poll, in which 49 percent of respondents suggested that they are either "not at all confident" or "not too confident" in the government's ability to protect their data, ranking higher only to social media sites.[18] The government's role in data privacy for citizens, however, is extremely complex due to the number of individuals and the amount of information entrusted to public institutions. Therefore, government organizations have a strong vested interest in protecting such information, including federal, state, and local governmental entities.

We therefore propose that because cybersecurity is a public good, it should be regulated as such through policies that promote sound cybersecurity practices. One potential solution is to require users to update their machines when new patches become available. Alternatively, stricter requirements may be placed on manufacturers of such products, including requirements

[15] *Ibid*. Pg. 18.

[16] *Ibid*. Pg. 14.

[17] Chalfant. Morgan. "Trump's budget proposal gives DHS $1.5 billion for cybersecurity". *The Hill*. March 16, 2017. https://goo.gl/d5zfWm

[18] Olmstead, Kenneth and Aaron Smith. "Americans and Cybersecurity". *Pew Research Center.* Jan. 26, 2017. https://goo.gl/wFqyhI

to download such patches in order to use the software. Alternatively, software manufacturers could require users to create secure passwords to prevent such intrusions.

There are, however, important questions about the legal and practical implications of requiring companies and users to engage in such activities, which lead to our research questions:

- *What cybersecurity doctrines are in use by local, state, and federal governments?*
- *What are their strengths and weaknesses and are there any viable alternatives?*

The remainder of the paper will investigate the role of government, industry and private citizens in an effective cybersecurity doctrine. §2 offers a summary of the cybersecurity problem. §3 describes the current cybersecurity doctrines and how select local and state governments employ them. §4 investigates the cybersecurity market, along with its failures. §5 addresses the role of government in public cybersecurity. Finally, §6 states our conclusions and offers areas for further research.

## 2.0 The Cybersecurity Problem

Before we identify the prevalent cybersecurity doctrines, it is necessary to describe the problem they are designed to mitigate. In its infancy, the internet was not designed with security as a primary concern. Many of the users were like-minded individuals focused on computer networking research, and as such, trust was implied. This is certainly not the case today, as the internet has grown into a worldwide construct with billions of users, many of whom have different motivations.

Cybercrime is an ever present part of the online experience, and protection of such sensitive information is a growing industry. According to a 2015 Forbes article, global spending on information security was estimated at $75 billion in 2014, and is expected to exceed $170 billion by 2020.[19] However, the vast number of malicious actors and the complexity of products in use make cyber theft an attractive avenue for criminals.

Robert Ghanea-Hercock, a British research scientist, authored the 2012 piece, “Why Cyber Security is Hard.”[20] The author argues that the various aspects of cybersecurity create “complex adaptive systems”, which are defined as “...systems that have large numbers of components, often called agents, that interact and adapt or learn.”[21] The nature of cyberspace is constantly evolving, and the complexity of cybercrimes, which often include crimes committed across borders and legal systems, further complicates this challenge. The increasing number of users worldwide, many of whom operate unsecured devices, requires action on the part of various actors.

Televisions, watches, appliances, and automobiles are becoming equipped with internet awareness that, on the surface, provides utility to end users. Unfortunately, the ease of use does not come without risk, and many of these devices lack sufficient built-in security measures. This opens the door to potential weaponization of internet devices at the hands of malicious actors.[22] While the “internet of things” is an exciting technological development, without proper security, the benefits of having an internet connected refrigerator are far outweighed by the potential risks.

[19] Morgan, Steve. “Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020”. *Forbes*. Dec. 20, 2015. https://goo.gl/2eG2s3

[20] Ghanea-Hercock, Robert. (2012). “Why Cyber Security is Hard”. *Georgetown Journal of International Affairs, International Engagement on Cyber 2012: Establishing Norms and Improving Security,* Pgs. 81-89. https://goo.gl/9ERUwg

[21] *Ibid*. Pg. 82

[22] Blumenthal, Eli and Elizabeth Weise. “Hacked home devices caused massive Internet outage”. *USA Today*. Oct. 22, 2016. https://goo.gl/aLSx27

Hacking activities are conducted in order to gain illicit access to a system that belongs to another individual or organization. The purpose for gaining such access may be to steal private or sensitive information, to manipulate data, or to install programs with a large array of potential uses, ranging from recording keystrokes of authorized users to launching denial of service attacks against commercial and government websites. The goal of cybersecurity is, therefore, to ensure that internet devices and the private data they store can be accessed and used solely by authorized users.

To understand the threats, it is helpful to think in terms of "known unknowns" and "unknown unknowns."[23] The known unknowns can come in the form of threats that are created by operating an unprotected machine. These threats are easily thwarted through the use of a robust patch management program. The unknown unknowns are harder to combat and generally come on the heels of a software patch release. Once a patch is released, there is a race between those working to take advantage of the newly identified security hole, and the propagation of the patch to fix it. Invariably, some users do not apply a patch immediately, either out of complacency or from an expedient desire to ensure that the patch does not break some other part of their system, and they are vulnerable to the efforts of those who seek to exploit the vulnerability.[24] These exploits are often packaged in self-replicating programs that copy themselves to unprotected computers, thus creating a chain of infections as they go along. If the security hole is one that, if exploited, results in the ability of an unauthorized user to gain

[23] Bambauer, Derek. (2014). "Ghost in the network". *University of Pennsylvania Law Review*, 162(5). https://goo.gl/xOKK8x

[24] U.S. Senate Committee on Homeland Security and Governmental Affairs. *Hearing on "Protecting America from Cyber Attacks: the Importance of Information Sharing"*114th Congress. 2015 (Written Testimony of Scott Charney Corporate Vice President, Trustworthy Computing, Microsoft Corporation)

administrative access, then the malicious software can be made to perform just about any function the operating system offers.

# 3.0 Current Cybersecurity Doctrines

There are several cybersecurity doctrines that seek to mitigate the risks the "unknowns" create through a variety of methods including risk management, prevention, and deterrence through accountability. Deirdre Mulligan, an associate professor at the School of Information at the University of California at Berkeley, and Fred Schneider, a professor of Computer Science provides at Cornell University, offer a succinct introduction the the current doctrines in use today.

## 3.1 Prevention

The doctrine of prevention aims to create systems that are completely free of vulnerabilities.  This includes the hardware, software, and human users. Such *absolute cybersecurity* is an unlikely achievement because of the nature of human activity towards error and the incredible difficulty in identifying every possible weakness in today's software.[25]

Gains may be made with the introduction of either voluntary or compulsory standards, but according to Mulligan and Schneider, no correlation between standards compliance and absence of vulnerabilities has been identified. This could be due to the fact that even the most comprehensive standards cannot take into account the rapid changes that occur in the technology

[25] Mulligan, Deirdre and Fred Schneider. (2011). "Doctrine for Cybersecurity." *Daedalus,* 140(4), Pgs. 70-92. https://goo.gl/AVcT9z

industry. Standards that attempt to address this might tend to stifle innovation because of the government's inability to keep the standards up-to-date with the pace of software advances.[26]

## 3.2 Risk Management

In the absence of absolute cybersecurity, it is sensical that system owners attempt to identify the risks and potential losses of a *de facto* incomplete cybersecurity. Once identified, these risks can be prioritized, and a dollar amount assigned to possible losses that could result from a breach. The value of potential losses would then dictate where cybersecurity dollars would be spent most wisely.

As Mulligan and Schneider suggest, this sounds like a sensible course of action, but there are some weaknesses to this doctrine. As mentioned above, there is no way to identify every weakness in a networked system, and therefore a complete picture of risks cannot be established. Also, if there is not a climate of information sharing, then an information asymmetry would exist between the possessors of available threat knowledge and those wishing to mitigate these risks.[27]

## 3.3 Deterrence

The doctrine of deterrence through accountability attempts to create an environment of cybersecurity through the threat of punishment or sanctions for commission of cybercrimes or data protection malfeasance. This applies to such federal statutes as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the proposed Cybersecurity Systems and Risks Reporting Act, which amends the Sarbane-Oxley Act of 2002 regarding activities of

[26] *Ibid.*, pg.78

[27] *Ibid.*

the Securities and Exchange Commission. A major problem with deterrence, however, is that it does little to enhance inherent cybersecurity, but rather incentivizes people not to commit a crime for fear of punishment.

## 3.4 Public Cybersecurity

### *3.4.1 Herd Immunity/Analog to Public Health*

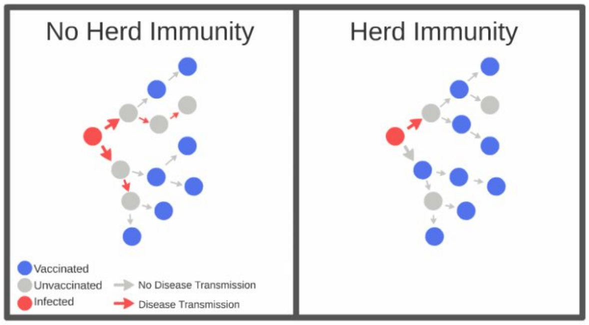
Research suggests that virus propagation through a computer network might behave much in the same way as a biological pathogen in an ecosystem. In a study that utilized telemetry data (n = 90+ Million) from the Microsoft Windows Malicious Software Removal Tool (MSRT), Fannie Lalonde Levesque, Anil Somayaji, Dennis Batchelder, and Jose Fernandez established a negative correlation between antiviral software use with virus infections.[28] They also found that unprotected computers in the proximity of protected ones enjoy a lower rate of infection.[29] This suggests that computer networks may behave like biological ecosystems which exhibit "herd immunity". This is a state achieved by an ecosystem when enough of the population becomes immunized to a pathogen so that propagation is minimized. **Figure 6-1 Herd Immunity** demonstrates this phenomenon. An infected host can only pass along a virus if it comes in contact with an unprotected host. If enough hosts are protected, both protected and unprotected hosts are less likely to encounter an infected host.

**Figure 6-1 Herd Immunity[30]**

[28] Fanny Lalonde Levesque, Somayaji, A., Batchelder, D., and Fernandez, J. (2015). "Measuring the health of antivirus ecosystems". *10th International Conference on Malicious and Unwanted Software* (*MALWARE*). pgs. 101-109. https://goo.gl/Hqmzr5

[29] *Ibid*.

[30] Patel, Kavita and Rio Harth. "What the anti-vaxxers are getting dangerously wrong". *The Brookings Institution*. Feb. 6, 2015. https://goo.gl/VO9CqQ



Levesque et al. recognize that there are some limitations and biases in the study, but their findings suggest an interesting topic for further research.

Using this analogy, it is not a big step to compare many of the public health practices to some of the tenets of Mulligan and Schneider's "Public Cybersecurity". Compulsory immunizations; quarantining of the infected; surveillance of ecosystems for signs of disease; maintaining diversity among populations; and boundaries, public education and training of professionals are all public health practices that have analogs in the realm of cybersecurity, as outlined in **Table 3-1 Public Health and Cybersecurity**.

**Table 3-1 Public Health and Cybersecurity**

| **Public Health Practice** | **Cybersecurity Analog** |
|---|---|
| Immunizations | Antivirus Software, Patching |
| Quarantines | Blocking Network Access |
| Monitoring Disease Spread | Network Scanning |
| Isolation | Firewalls |

## 3.5 Implementation

While each of the first three doctrines described above do not individually present a comprehensive approach to cybersecurity, when combined, they frame the strategy that is used by nearly every individual and organization who is serious about protecting their data and networks. Private citizens work towards prevention by maintaining their systems with security patches and practice risk management by paying for encrypted cloud services to store their data. The also rely upon federal statutes to ensure accountability for their personal data held by local, state, and federal governments. The same formula applies to organizations and governments, although they may employ large information technology (IT) security teams to work towards prevention and to create risk management programs that are as accurate as they can be, despite the information gap.

## 3.6 Case Study - The Commonwealth of Virginia

Kate Jackson, Secretary of Technology for the Commonwealth of Virginia, provided an insightful interview regarding the state's approach to cybersecurity. Shortly after taking office, Governor Terry McAuliffe identified cybersecurity as a focus of his administration. Understanding that states have a mandate to protect the large amount of personal data (birth and death records, driver's licenses, property records, etc) in their charge, he made it the goal of his administration to get a better understanding of how and where Virginia stored and protected this information, and to make cybersecurity an upfront issue throughout the state.

To this end, the Executive Office of the Governor of Virginia recently completed an audit of all executive branch information systems that contain personally identifiable information (PII) of the residents of Virginia.  Using the results of this audit, they then created a risk management program that accounted for the sensitivity of the information being protected and applied a priority rating system that helped them to identify the agencies with the most risk and the best ways to spend state cybersecurity dollars.

The result was a program that employed non-traditional approaches to include Computer Information Security Officers who were either detailed permanently to agencies that housed large amounts of PII, or regional Chief Information Security Officers who service the smaller agencies only in need of periodic support, to ensure the health of their networks. Additionally, the Governor's office enlisted the help of the Virginia National Guard to conduct cybersecurity audits of executive office agencies.

The Governor's office took on the challenge of cybersecurity education as well. Cyber VA is an information repository where users from many sectors can access the current thinking on cybersecurity. Rather than recreate the wheel, Cyber Virginia's aim is to collect the work of government and industry together on one site where Virginia residents (or anyone) can go to learn about cybersecurity best practices. The state is also actively involved in increasing funding for higher level IT education, and is working to implement a tuition for state service program that will hopefully help to

# 4.0 Cybersecurity Market

## 4.1 Description of Market

There are many different components of the cybersecurity market. Private companies produce cybersecurity products in the form of antiviral software, firewalls, and routers. Other firms offer cybersecurity services to individuals and firms. These products and services operate on the free market and are by all indications a booming industry. The following chart utilizes the standard market goods grid to highlight some of the different public and private goods cybersecurity products and institutions that comprise the market. It is noteworthy that the public goods quadrant is filled with goods that deal in information, and the other quadrants contain goods that have some sort of marketable product or deliverable in the form of services, funding, software, or hardware. This representation can help to determine the market failures afflicting cybersecurity.

**Table 4-1 Cyber Security Market Goods**

| | **Non-Rivalrous** | **Rivalrous** |
|---|---|---|
| Non-Exclusive | Public Goods<br>Public Cybersecurity (institution)<br>Security Threat Information<br>Security Best Practices | Common Goods<br>Federal Cybersecurity Subsidies |
| Exclusive | Club Goods | Private Goods<br>Cybersecurity Services<br>Formal Cybersecurity Education<br>Commercial Antivirus Software<br>Commercial Firewalls |

In theory, a public good is simple to understand, but identifying real world examples is more challenging. A public good is something that is both non-excludable and non-rivalrous, meaning it is free for use by all and is not depleted with use. The perennial example of this is national defense (assuming, for our purposes, that the "public" is the set of all people living within the borders of a specific country). One can freely consume the security provided by the military, and the individual's use does not deplete the amount of national security available to the next person.

If cybersecurity is to meet the requirements of a public good, it must be both non-excludable and non-rivalrous. Much like national defense, the umbrella of a state of cybersecurity is available to all, and assuming free ridership is not abnormally high, one person's use of the state of relative safety from attacks provided by cybersecurity does not preclude another from the same protections.

A collective practice of implementing cybersecurity best practices could make it less appetizing for malicious actors to pursue phishing schemes or to build self replicating viruses or malware, and as a result the entire network would become more secure. This is the real world effect of the "herd immunity" that was previously discussed.

To reinforce its status as a public good, cybersecurity suffers from a free-rider problem. Individuals can choose to not contribute to public cybersecurity by using weak passwords, not patching their personal computers, or not securing their home routers, and yet can still benefit from the state of cybersecurity provided by the rest of the collective.  The rational actor could decide that because everyone else is practicing good cybersecurity, there is little risk of attack, and it is therefore not worth the effort or expense to implement best practices alone.

This does not pose a significant problem to the collective, as long as the instances of free-ridership remain low. If free-ridership grows, then the ability to maintain the herd immunity decreases and the number of infections increases. Along with this increase comes negative externalities in the form of transmission channels that are clogged with malicious traffic and a rise in infection attempts, both of which raise the required levels of diligence on the part of those who practice good cybersecurity.

## 4.2 Cybersecurity Market Failures

In the case of cybersecurity, users of commercially available products benefit from the ability to use networks to obtain and exchange information. Yet each user who chooses to take part in the network also bears a certain responsibility. Microsoft Windows is a standard operating system that is used by billions of users and organizations globally. In order to maintain security on Windows machines, Microsoft regularly and frequently releases software patches intended to address security vulnerabilities. Such patches prevent individual machines from affecting a network of computers.

Government agencies and organizations regularly download and install such patches on computers. While individual users have a vested interest in downloading and installing the patches on their own machines, many fail to do so, thus leaving their machine susceptible to malware or phishing. This ultimately affects other users on a network and ultimately contributes to the cybersecurity vulnerabilities across networks. This risk has only increased over time as more individuals have access to networks and devices. Moreover, Microsoft no longer supports legacy products that were the industry standards years ago, such as Windows XP, although many of machines that run such products are still in use both domestically and internationally.

Governments exist, in part, to compensate for market failures. A market failure occurs when there can be improvements made to the efficient distribution of goods that does not degrade the distribution to an individual group or groups. Because public cybersecurity is a public good, and government policies are intended to address potential market failures, government policies can be crafted to promote good public cybersecurity practices. In the case of air pollution, states are required to follow specific National Ambient Air Quality Standards by the U.S. Environmental Protection Agency to protect the air quality of that state, and also that of nearby states. Similarly, individuals are required in many states to have their cars inspected periodically to ensure that they meet certain safety and emissions requirements for their own safety and benefit, as well as for others. Many policies, therefore, are intended to promote both the individual interests and those of other affected parties.

Private actors are not the only entities that can have a negative effect on collective cybersecurity. The incredible complexity of today's computer software makes it difficult, if not impossible, to accurately identify every security vulnerability. The interaction between software, hardware, and human users provides for a tightly coupled and complex system that experience failures.

It is therefore not enough to declare a general cybersecurity market failure due to an increase in cybersecurity incidents. The individual components of public cybersecurity must be evaluated. The following table extends the components listed in **Table 4-1 Cybersecurity Market Goods** to include potential market failures.

| **Table 4-2  Cybersecurity Market Failures** | | |
|---|---|---|
| **Component** | **Type of Good** | **Potential Market Failure** |
| Public Cybersecurity | Public | Public Good/Inefficient Distribution |
| Security Threat Information | Public | Information Asymmetry |
| Security Best Practices | Public | Information Asymmetry |
| Software Vendors (Antivirus/OS) | Private | Negative Externality, Non-Competitive Markets |
| Cybersecurity Services | Private | Negative Externality |
| Formal Cybersecurity Education | Private | Information Asymmetry |

Security threat information is one of the most valuable assets available to combat cyber attacks. Without this knowledge, software vendors do not have the information necessary to correct flaws in their products, companies cannot make financial decisions based on risk analysis, and individuals do not have the motivation to secure their personal IT systems. This information asymmetry can be partially alleviated through the construction of information clearinghouses that are a partnership with industry and government.

Security best practices are another public good that can suffer from an information asymmetry market failure. Consumer level examples of best practices are the use of strong passwords, proper identification and response to phishing attempts, and consistent patch management for personal IT systems. Commercial examples are the proper configuration of data servers, network topology construction, and user access management. This body of knowledge is compiled over time as a result of lessons learned and proactive security planning.

Cybersecurity services and professionals can be hindered by the same lack of security threat information as other parts of the industry. Since they are unable to completely identify the the threats faced by their customers, they are unable to provide a complete security service or guarantee.  In this sense, there is a negative externality of risk that they are passing along to their customers in the form of losses suffered in the event of breach due to a previously unknown threat.

Modern software is of such complexity that renders it expensive and difficult to accurately identify potential weaknesses and avenues for attack prior to release. This is evidenced by the patches that vendors offer to update their software, and while patch programs show a good faith effort on the part of developers to ensure that their product is as secure as possible, there still exists a market failure in the form of negative externalities. The software vendors are unable to identify each security hole in their products, but they sell such products anyway, thus passing the risk of breach along to their customers who will be forced to internalize the costs of any breaches that utilized weaknesses in the software installed on their machines, even if they stay current with security patches.

## 4.3 The Role of the Private Sector

The public sector has frequently collaborated with the private sector to promote enhanced cybersecurity practices, as outlined in FISMA. While this has produced many innovations in the field, there are also limitations to this relationship. Amitai Etzioni, a professor at the Elliott School of International Affairs at George Washington University, suggested in his 2014 piece, “The Private Sector: A Reluctant Partner in Cybersecurity”, that both the George W. Bush and

Barack Obama administrations were reluctant to introduce strict cybersecurity measurements for industry.[31] In his view, however, the private sector has multiple motivations for not adopting stronger measures. The author cites that there exists an economic component for this, as firms may be reluctant to adopt practices that increase their costs and their regulatory burden. The author also cites reluctance from organizations such as the United States Chamber of Commerce and The Heritage Foundation.[32]

Etzioni also suggests that private sectors actors may oppose added cybersecurity measures as such measures may be harmful for the purposes of innovation or for their security. In addition, he suggests that some actors may view cybersecurity as a responsibility of the government. He further suggests that mandated reporting of incidents may open organizations to negative media attention and legal action from affected parties.[33] Etzioni specifies that the federal government has investigated ways to incentivize industry, such as the offering of cybersecurity insurance and grant money, yet he suggests that the government's reluctance to place stricter requirements on industries has many implications for national security and for the nation's infrastructure. He also suggests that because the government relies on many firms to provide computer systems and contractual services, firms have added responsibility to promote safer practices.

The work of Etzioni and others suggests that there are several legal and political challenges that complicate the feasibility of such policies. Organizations have many interests, and the political mechanisms that exist allow for actors to promote and protect their interests.

[31] Etzioni, A. (2014). "The Private Sector: A Reluctant Partner in Cyber Security". *Georgetown Journal of International Affairs*(4), 69-78. https://goo.gl/WWhhrJ
[32] *Ibid*.
[33] *Ibid*.

Regulation, in general, can create many burdens for industries and individuals, and the current administration of President Donald Trump has promoted deregulation as a means to reduce costs for actors. Various historical and cultural aspects help to frame the notion that government is best suited to allow market forces to drive and protect industries. These political challenges, therefore, pose many questions regarding the government's role in protecting cybersecurity, which require investigation as to the basis by which government intervenes to address perceived market failures.

# 5.0 Role of Government in Public Cybersecurity

There is a gap between the cybersecurity market failures and the ability of current cybersecurity doctrines to combat them. For instance, in the case of information asymmetry of known threats, none of the three doctrines will create openness between software developers, security analysts, and government. They will not incentivize consumers to patch the home machines or use strong passwords, nor will they incentivize developers of IT goods to work to build stronger security into their products.

## 5.1 Possible responses to cybersecurity market failures

If an effective public cybersecurity doctrine is to be established, government will need to intervene to help correct these market failures.  Options are available to either incentivize or coerce industry and individuals to practice better cybersecurity. Regulation may focus on moving the state of our networks, both private and public, to one that is capable of achieving herd immunity. This collective approach could take the form of laws that parallel those of public health, requiring users of internet aware devices to ensure that their devices are patched and protected by antiviral software, like a vaccination.  Computers could be required to send encrypted “health certificates”, like shot records, that ensure that they are secure to the level of an agreed upon standard before being given access to external resources, and those that do not pass the health test could be denied access to the network, like a quarantine.[34]

The literature, our interview subjects, and simple observation suggests that there are several forms of intervention the government might use to address the cybersecurity market failures. Working towards a goal of collective cybersecurity, the government could focus on both the provision of the public goods previously identified and work to add more consumer protections to the private goods for sale in the marketplace.

Government might work to enact regulations to compel software vendors to force the use of already built-in security measures such as two factor authentication or mandate that firewall protection and malware or antivirus scanners be updated before shipping and enabled by default. One of the authors of this paper recently purchased a new Windows 10 laptop that was delivered with antivirus and malware definitions that were one year old. AV-Test, an independent IT research organization, estimates that there were more than 120,000,000 new instances of malware identified during that time[35] that would not have been included in the malware definitions for the new laptop at time of shipping. Certainly, having up-to-date antivirus definitions is not sufficient.

[34] Mulligan, Deirdre and Fred Schneider. (2011). “Doctrine for Cybersecurity.” *Daedalus,* 140(4). https://goo.gl/ZOF194

[35] “Malware”. *AV-Test GmbH.* Last updated March 20, 2017. https://goo.gl/vGLbjJ

Mulligan and Schneider suggest offering incentives to or compelling Internet Service Providers (ISPs) to block internet access to computers that show signs of being unprotected until they are secured by their owners.[36] This, however, raises an interesting question about whose traffic is it that is flowing over their networks: should ISPs be held responsible for the spread of viruses? Recent developments in the area of net neutrality would suggest that they desire more control over how to manage bandwidth, but will they also take more ownership of the health of the collective network? Additionally, ISPs are in the business of selling bandwidth, and like it or not, malicious traffic consumes bandwidth. This contributes to a slowing down of legitimate traffic, compelling end users to consider upgrading their ISP service package. That's not to suggest that ISP's are complicit in the spread of malware, but a reduction in the amount of traffic caused by malware could result in a net reduction of demand for their services.

At the consumer level, end users could be held accountable for the state of their systems. Much in the same way that automobiles are required to undergo periodic safety inspections, personal computers and internet devices could be required to transmit a "health certificate"[37] to the ISP or individual websites before being given access to remote resources. This certificate could be the data collected by system scanning tools that report on patch status, malware protections, or antivirus definition dates. But end-user consumer cybersecurity practices are of importance on an education front as well.

It is not enough to have a patched computer; consumers must possess a certain amount of technological knowledge if they are to contribute to the collective cybersecurity. Public education is another area where government may intervene to alleviate one of the cybersecurity

[36] Mulligan, Deirdre and Fred Schneider. (2011). "Doctrine for Cybersecurity." *Daedalus,* 140(4). https://goo.gl/jrWC9G

[37] *Ibid.*

market failures. Levesque et al. noted that while varying education levels correlated strongly to cybersecurity in some countries, this was not the case in the United States. The American population as a whole receives sufficient compulsory education for this variable to not play a meaningful role in cybersecurity in the United States, meaning that it should be possible to develop a public awareness campaign aimed at the average high school graduate.

Our conversation with an individual who is both a cybersecurity professor and an industry expert, who requested to remain anonymous, provided us with unique perspectives regarding potential solutions to the cybersecurity question. The respondent concurred with the idea that we can look at cybersecurity as a public good, and noted that certain states, such as New York and California, have taken a lead in this area. Yet the respondent also pointed out that the private sector has already introduced reforms to address cybersecurity concerns, such as the integration of built-in antivirus software into Microsoft Windows 10, and that the best solutions may actually be at the vendor level.

Another recommendation that the respondent suggested is a labeling system in which products would be labeled for their ability to defend against cyber threats, as this would shift the incentive structure for manufacturers and developers. Currently, consumers can compare automobiles based on the National Highway Transportation Safety Administration’s star rating system, which is placed on the window sticker of new vehicles. Consumers therefore have more information because of this rating and can decide whether the vehicle’s safety is a priority that will guide their purchase decision. A similar system for devices and computers may enhance consumer awareness and could potentially incentivize companies to produce better products in order to increase the attractiveness of the device and remain competitive.

The respondent did, however, point out many of the challenges of implementing such regulations, due in part to the inadequate numbers of seasoned professionals within the government. This poses an administrative challenge, as it may be difficult to enforce certain policies if there are not enough experts to determine what constitutes a violation or a threat. Secretary of Technology Jackson, however, outlined a program that Virginia is piloting to offer college scholarships to future IT professionals in exchange service to the state upon graduation. The professor also pointed out that there are certain industries that perform better at cybersecurity than others. Identification and further studies of best practices employed by industries may hold potential solutions to the problem.

Our respondent further argued that an education campaign may help to address the threat, and can be integrated into the education system. Yet the individual also pointed out that the limited resources available make implementation of programs and regulations difficult. As states and legislators contend with crises like the opioid epidemic, budgeting priorities do not time center on this issue at this time. As echoed by others, a major incident may spark legislators and the public to take greater action, yet at the moment, cybersecurity is not a top priority for many.

While the government has taken action in some ways to protect public information entrusted to government agencies, there still is much work to be done in the realm of collective cybersecurity. It is possible that the true threat will not be publicly understood until the occurrence of a large scale incursion and/or loss life occurs due to cybercrime. This could come in the form of disruption of public utilities, as was seen in Dallas in April 2017.[38]

[38] Simpson, Ian. "Computer hack sets off 156 emergency sirens across Dallas". *Reuters*. April 9, 2017. https://goo.gl/T3hdvO

David Jordan, the Chief Information Security Officer of Arlington County, Virginia offered some thoughts on how government might contribute to better cybersecurity. He is a strong proponent of working to require that security be "built-in" to private-public IT contracts and internet products, and makes the observation that in the end, it's cheaper to build in security rather than try to mitigate the threats after the fact. This sentiment is mirrored by Ghanea-Hercock, who suggested in 2012 that computer systems should be designed for resilience, although this may pose high research and development costs.[39]

Mr. Jordan also raised the issue of organizational change within local governments to a condition where cybersecurity is promoted to the level of public safety. He has gone on the record in the past to implore governments to increase their cybersecurity spending, both as a means to prevent a calamitous hack of a public water system, energy grid, or even something as mundane as a traffic light system, but also as a means to better protect the expensive personal data of citizens. To achieve this, he says, budgeting for the nice-to-haves must give way to a more comprehensive view of cybersecurity with funding to match.

In Mr. Jordan's view, cybersecurity doesn't begin and end with government and industry. End users also play an important part and have an obligation to the collective to employ strong cybersecurity practices. Assuming that there is an interest on the part of the public, issues exist that confound any efforts to contribute to the public good. Issues in availability of education (school students receive cybersecurity education, but elderly users are often left behind), and patch reliability (e.g., windows patches can sometimes break other software applications

[39] Ghanea-Hercock. (2012). "Why Cyber Security is Hard". *Georgetown Journal of International Affairs, International Engagement on Cyber 2012: Establishing Norms and Improving Security*, Pg. 87. https://goo.gl/1WzU6i

installed on computers, causing hesitancy to install the patches until the potential damage is more well-known) can serve to reduce the amount of cybersecurity public good produced by the public.

In the end, Mr. Jordan believes that everyone has a role in the production of cybersecurity, and that in general, federal, state and local governments should spend more budget dollars in this arena. He suggests that we need to both devise more secure ways to live with the current condition of cyber-insecurity, but continue on a track of continual improvement. Like our other interviewees, he holds a view that it may take a tragic cyber event to trigger an adequate focus on the subject, which will in turn produce more funding to protect the sensitive infrastructure and information that resides in or is controlled through cyberspace.

## 5.2 Public Administration Considerations

Many of the themes identified in this paper are of interest to Public Administrators. Issues of collective good, market failures, government intervention in a market, policy development and implementation, and avoidance of constitutional transgressions can be found in a discussion of Public Cybersecurity. Below are listed some of the possible issues new cybersecurity regulations may confront in the legal, political, fiscal and managerial arenas. These examples are the result of analysis of the problem using a review of the themes we were exposed to during the course of study in our MPA programs.

### *5.21 Legal Considerations*

- There are privacy issues with government scanning of IT devices, but following the public health comparison, the Supreme Court of the United States upheld mandatory vaccinations in *Jacobson v. Massachusetts*, so it appears that if a case can be made for the public good, this might not pose a legal threat.

- Potential legal action against software developers and hardware manufacturers if manufacturers are required to disclose data vulnerabilities.
- The existence of international cybercrime across borders and legal systems.
- Required global coordination and cooperation due to a lack of an strong international framework.

*5.22 Political considerations*

- Free market intervention and the potential for government overreach into market correctable areas.
- Forced compliance of vendors that provide contractual services to governmental organizations may create political tensions.
- Privacy concerns on the part of users and suppliers.
- Organizational interests and compliance costs.
- Coordination efforts with domestic and international jurisdictions.

*5.23 Fiscal considerations*

- Mandatory public cybersecurity requirements may raise the cost of ownership or use.
- The complexity of software makes security compliance expensive.
- Added enforcement costs for the government.
- Increased budgets to account for added administrative costs.

### *5.24 Managerial considerations*

- Agency responsibility for managing public cybersecurity concerns.
- Role of state and local jurisdictions.
- Data submission requirements and the additional administrative burden.
- Performance and effectiveness measurements. The methods for measuring the effectiveness of government programs is a complicated and hotly debated topic, and this is not made any simpler by the complexity of the cybersecurity market.

## 6.0 Conclusions and Areas for Further Research

In this paper, we identified and addressed some of the market failures surrounding cybersecurity. There are aspects of the market that can be considered public goods (overall state of cybersecurity, threat information sharing), and as such, are being underproduced. There are other areas that create public goods which either suffer from information asymmetries or create negative externalities (unsecure software products). Through careful policymaking, the government might be able to help alleviate these market failures, which will in turn create a heightened level of collective cybersecurity. As with any new policy, there will be legal, political, fiscal, and managerial concerns to contend with, but these have been successfully addressed in the past with other issues pertaining to public health and security. It is not beyond the realm of thinking that a public security doctrine with both coercive and incentivizing aspects could be developed that enhanced the collective good.

## 6.1 Area for Further Research - Global Governance

While this paper focused on the cybersecurity problem as it relates to the United States, there is a much larger issue of global cybersecurity that will, at some point, need to be addressed. Even if the U.S. managed to reach a state of herd immunity for the systems within its physical borders, much of the world's internet traffic transits the U.S. via international data lines. Work to reduce the number of malware instances on domestic networks could be negated by traffic from less cyber-aware nations. Levesque's work suggests that country level variables have an effect on cybersecurity, and their interactions with the U.S. network raises questions of global governance and development[40]. This extends the conversation out of the technical arena and into that of foreign affairs. For future research, it may be interesting to further investigate how the findings of this paper might apply to a "Global Public Cybersecurity Doctrine".

Government, however, currently plays a vital role in this area, and its cooperation with the private sector allows for potential market-based solutions to the problem. Corporations and vendors may be incentivized to sell safer and better products if customers perceive the value in buying something that protects their data, in the same way that individuals purchase vehicles that may cost more but have a five-star safety rating from the National Highway Traffic Safety Administration. Government may employ alternative solutions, such as labeling requirements, that can promote industry to create better and safer products.

Additionally, the government may utilize the contracting process to leverage manufacturers to create industry-wide enhancements by setting minimum standards for

[40] Fanny Lalonde Levesque, Somayaji, A., Batchelder, D., and Fernandez, J. (2015). "Measuring the health of antivirus ecosystems". *10th International Conference on Malicious and Unwanted Software* (*MALWARE*). pgs. 101-109. https://goo.gl/Hqmzr5

procurement. This is challenging, as certain manufacturers are sole providers of major software products, such as Microsoft Windows. At this point, however, it seems unlikely that the federal government, can feasibly produce its own operating systems and hardware solely for public sector use, and providers therefore may carry the burden of meeting stricter standards to maintain their relationships with public organizations.

In addition, statewide and local efforts to promote safer cyber practices through user education and public awareness campaigns may prove valuable to promote the industry, as we have seen in the state of Virginia. With the complexity of budgeting, however, such policies may be viewed by the public and decision-makers as less important than other issues. Finally, cybersecurity practices can be promoted through the continual efforts of the federal government to prioritize cybersecurity as a national security and defense issue, which was the case during previous administrations and will likely be a focus of the new presidential administration.