



## **Cybercrime as a Market Failure: A Welfare Economics Framework for Understanding Consumer Surplus, Producer Surplus and Deadweight Loss in the Digital Economy**

**Dr. Samprit Chakrabarti**

Dean, School of Business, Adamas University,

Email id: [samprit.chakrabarti@gmail.com](mailto:samprit.chakrabarti@gmail.com)

ORCID: 0009-0004-5013-7205

**Dr. Sarojkant Singh\***

Assistant Professor, School of Business, Management, Strategy, Adamas University,

email id: [sarojkant.singh1@adamasuniversity.ac.in](mailto:sarojkant.singh1@adamasuniversity.ac.in)

ORCID: 0000-0002-4319-8673

**Dr. Raja Ghosh**

GM (F&A) Corporate Planning, WBSEDCL, email: [rajaghosh70@rediffmail.com](mailto:rajaghosh70@rediffmail.com)

ORCID: 0000-0002-7861-6580

**\*corresponding author**

**Received:** 12 May 2026

**Accepted:** 14 Aug 2026

**Published:** 06 Oct 2026

### **Abstract:**

Digital technologies have revolutionised global commerce, communication and delivery of services, and similarly have increased the nature and complexity of cybercrime. Most research on cybercrime focuses on direct monetary losses, cybercrime security spending, loss of productivity, and macroeconomic effects, and overlooks the ramifications of economic welfare. It is this shortcoming that this paper seeks to correct by outlining a novel framework for welfare economics analysis to conceptualise cybercrime as a market failure which causes a loss of consumer surplus, producer surplus, and overall social welfare via the deadweight loss. This paper is based on welfare economics, information asymmetry theory, externality theory, and builds a conceptual model on how cyber threats destroy consumer trust, create transaction costs for consumers, force companies to invest in defence technologies, and ultimately derail the equilibrium of digital markets. The framework is illustrated through sample scenarios of cybercrime in the context of tourism booking fraud, social media marketing fraud, gaming scams, WhatsApp account compromise and cyber grooming, to show how these attacks have economic impacts beyond any financial losses. The results indicate that cybercrime represents hidden welfare costs in the form of disincentive effects on mutually beneficial digital transactions, on market participation and on the cost of doing business for legitimate enterprises. This means that the amount of damage associated with conventional estimates of financial loss, which include only the actual monetary losses, vastly underestimates the true social costs of cybercrime. This proposed framework adds to the growing field of the economics



of cybersecurity by combining the welfare-economic and the digital forensic/ cybersecurity points of view, providing a holistic view to policymakers, business and researchers in determining the overall economic impact of cybercrime. This study ends with the identification of avenues for empirical testing and the creation of a Cybercrime Welfare Loss Index to aid evidence-based cybersecurity policies and digital market regulations.

**Keywords:** Cybercrime; Welfare Economics; Consumer Surplus; Producer Surplus; Deadweight Loss; Digital Markets; Market Failure; Cybersecurity; Digital Forensics; Consumer Trust.

## Introduction:

The electronic transformation of commerce, financial services, communication and public administration has had a marked positive impact on the economic productivity and convenience of consumers. At the same time, however, this digital transformation has created an increased attack surface for the cybercriminals that have led to significant economic and societal costs. Global cybercrime now takes the form of a complex transnational organization which includes ransomware, phishing, identity theft, financial fraud, manipulation of social media, and attacks on critical infrastructure (Anderson et al., 2013; Moore, Clayton, & Anderson, 2009). Therefore, cyber security is no longer considered as a mere technological problem, but more and more an economic and public policy problem that needs interdisciplinary study (Gordon & Loeb, 2002).

Previous studies have focused on quantifying the cost of cybercrime in terms of direct financial losses, incident response costs, cybersecurity investments, productivity costs, and the macroeconomic costs and implications (Biener, Eling, & Wirfs, 2015; Romanosky, 2016). These studies can give a good idea of the costs of a cyber incident, but are less informative about the welfare costs associated with decreased trust in a specific network, higher business operating costs, or fewer transactions conducted in digital markets. The distortion it creates is like the classical market failures due to lack of information, negative externalities and inefficient market outcomes (Akerlof, 1970; Stigler, 1961).

This study fills this gap by developing a framework of welfare economics that views the occurrence of cybercrime as a cause of reduction of consumer surplus, producer surplus and social welfare, which leads to the formation of dead weight loss. The paper bridges the gap between welfare economics and cybersecurity/digital forensic views, providing a novel conceptual framework that can be used to consider the hidden economic costs of cybercrime beyond the traditional financial loss estimates, and thus to the economics of cybersecurity and digital market policy.

## 2. Literature Review

As digital technologies have permeated consumption, production, financial transactions and service delivery, the economic impact of cybercrime has become a growing concern. However, previous studies have typically taken place in isolation. The economics of information security explores the incentives for investing in the information security space,



costs of cyber incidents; digital-market research explores trust, perceived risk, and technology adoption; and digital-forensics research focuses on evidence collection, investigation, attribution, and recovery. They help to understand the effects of cybercrime, but have rarely been incorporated into a welfare-economic analysis that explicitly links cybercrime to changes in consumer and producer surplus, deadweight loss, and social welfare. This paper stems from these flows and introduces cybercrime as a possible cause of market failure in the digital economy.

## **2.1 Economics of Cybercrime, Welfare Economics and Market Failure**

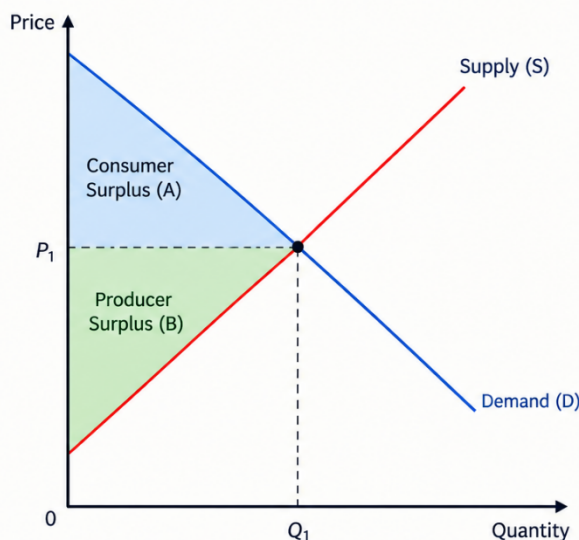
First one can understand the economics of cybercrime by looking at the economics of information security. Information security is a resource-allocation challenge in which firms have to decide how much to invest to minimize the risks and impact of security events. Some researchers, such as Gordon and Loeb in 2002, have shown that the concept of security investment has to be considered in terms of the expected losses from an information-security attack, not merely as a cost of technology. Likewise, Böhme and Moore (2012) believe that information-security issues have unique economic features, as the economic value of information is hard to assess, risks are uncertain, and the economic decisions made about security have multiple actors.

However, cybercrime poses another economic challenge since the impact of an incident goes beyond the immediate organisation. Anderson, et al (2019) show that the costs of Cybercrime include direct financial losses, costs of prevention, costs of recovery, costs of investigation and opportunity costs. These costs have an impact on both sides of a digital market. Consumers can suffer from financial damages, disruption and privacy breaches, and a diminished appetite for transactions, and firms can spend money on cybersecurity, incident response, compliance, recovery, insurance and reputation management.

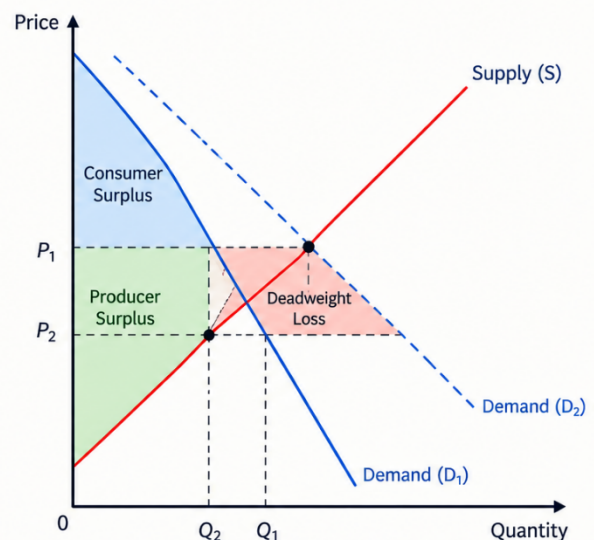
These effects can be combined in a useful theory, namely welfare economics. In a competitive marketplace, consumer surplus and producer surplus are the benefits the buyer and the seller derive from an exchange in the market. Consumer surplus is created when consumers are willing to pay more than the current market price and producer surplus is created when producers earn a price higher than the minimum price they would need to supply the product or service (Marshall, 1890). A combined surplus under conditions where market prices capture the relevant cost and benefits is a more traditional measure of market welfare.



**Figure 1. Digital Market Welfare under Secure Conditions**



**Figure 2. Cybercrime-Induced Market Distortion and Deadweight Loss**



This baseline is shown in figure 1. A digital market is relatively secure, and the actions of demanders and suppliers lead to an equilibrium price and quantity. Consumer surplus is the area between the demand curve and the price above the equilibrium price and producer surplus is the area between supply curve and the price below the equilibrium price. The combined surplus is the sum of the surplus from market transactions. The figure is thus a threshold that can be used to compare the deterioration of the welfare resulting from cybercrime.

The problem with cybercrime is that it can disrupt the benchmark by creating conditions that are not fully reflected in the market's pricing. This is especially relevant with regard to information. When buyers are unable to sufficiently distinguish between high and low quality products, uncertainty can change the nature of market participation, and may be detrimental to an efficient exchange process, as Akerlof (1970) showed. Digital transactions exacerbate this issue as people may not be able to see how secure a platform is, how authentic the seller is or how they use the personal information they collect or how likely they may be of being frauded before they part with their money.

Cybercrime could therefore have similar impacts to market failure. Conditions determining mutually beneficial transactions can change due to information asymmetry, negative externalities, higher transaction cost, and risk perceptions. Pigou's (1920) welfare-economic approach to external costs is the seminal work, whereas the distinct focus on transaction costs of Coase (1937) and Williamson (1985) has been pivotal in organisational and efficiency aspects of economic exchange. Cybercrime can thus be defined for a digital market as another cost and risk source which is not necessarily visible in the apparent market price.

The implication of this is that the welfare impact of cybercrime is not limited to the amount of money that's stolen or damaged in the event. Consumers might shy away from using digital transactions and companies might cut back on their use of digital markets due to heightened



risk, so that the transactions that would have been beneficial to both parties may not happen. This offers the theoretical foundation to ponder deadweight loss as an important albeit underdeveloped aspect of cybercrime economics.

## 2.2 Consumer Trust and Digital Markets

Trust is a key mechanism that can impact the behaviour of digital markets in the context of cybercrime. Some of the uncertainties of digital transactions are quite large compared to many traditional transactions, such as: Who is the other party—the identity of the other party; security of the payment system—the security of the payment systems; handling of personal data—how personal data is handled; quality or authenticity of the product or service—the quality or authenticity of the product/service. Both the perceived risk and trust are shown to be important factors in the acceptance of electronic-commerce by Pavlou (2003), and by Gefen et al. (2003), who incorporate trust into technology-acceptance explanations of online purchasing behaviour.

These mechanisms make it easier to fight cybercrime. Consumers' perception of vulnerability can be heightened by fraud, identity theft, phishing attacks, attacks on payment systems, data breaches, ransomware and social-engineering attacks. Knowing about a cyber incident may also impact consumer willingness to provide information, make online payments, use different platforms, or use new online services, even if the individual customer isn't directly impacted by a monetary loss. Therefore, the economic impact of cybercrime could be manifested by behavioural responses, as well as the immediate monetary damage.

It is important for welfare analysis because it allows for a distinction between the two. A direct economic cost is incurred by a consumer who keeps on buying and suffering a financial loss. If someone does not make a digital transaction due to a perceived risk of cyber, then this is a different kind of welfare effect – a mutually beneficial transaction that simply doesn't happen. The latter mechanism is more apt to the concept of dead weight loss as the value which could have been realised for both consumer and producer is not realised.

The scale of this mechanism is also expanded with digitalisation. Goldfarb and Tucker (2019) define digital markets using the following characteristics: almost zero marginal reproduction costs, the extensive use of data, and network and platform effects. These attributes can bring significant rewards to digital involvement, but can also reduce the effects of losing trust. The implications of diminished participation on a platform could be more than just a few transactions, they could be the entire platform ecosystem of users, sellers, advertisers, financial institutions, service providers, etc.

In Figure 2, we further the idea established in Figure 1 that there is a market distortion driven by cybercrime. A rise in the perceived cyber risk may cause consumers to be less willing to participate, shown graphically as a decrease in the demand for it. As a result, the quantity at equilibrium will drop from a safe market quantity to a lower quantity. Consumer and producer surplus are both decreased, and the trades that are not made are due to lost gains from trade. The resulting triangular area is the concept of the loss of mutually beneficial digital transactions and is called the dead weight loss.



Therefore, it is not an accurate measure of cybercrime-induced deadweight loss, but rather a conceptual welfare representation, as can be seen in Figure 2. It aims to link the behavioural consequences that are described in the digital-trust literature to the concepts of welfare in economics. This connection is of importance in terms of theories that connect cybersecurity and market efficiency studies.

### **2.3 Cybersecurity, Digital Forensics and Welfare Restoration**

The supply side effects of cyber-crime contribute to the demand side effects with regard to trust. There are several ways in which organisations respond to cyber risk, such as cybersecurity investment, monitoring, compliance, incident response, insurance, recovery and technological upgrading. Gordon and Loeb (2002) describe information-security investment as an economic choice between the loss and the allocation of resources, and Anderson et al. (2019) illustrate how cybercrime has an impact beyond the immediate victim that causes social and economic damages.

Even if an organisation manages to keep a big breach at bay, these costs can still decrease producer surplus. Security, compliance and monitoring and preparedness for incidents have an opportunity cost relative to other activities that could be done with that resource, such as production, innovation, marketing or expansion of service offerings. Other expenses can be incurred after an incident such as investigation, system restoration, customer compensations, legal proceedings and reputation damage. So cybercrime can impact producer welfare both in terms of actual losses, and in terms of the resources needed to deal with cyber risk.

Digital forensics takes this relationship to a whole new level. Digital forensic processes are used to facilitate the identification, preservation, examination and interpretation of digital evidence, and can help with incident reconstruction, attribution, loss assessment, and legal matters (Casey, 2011; Carrier, 2005). In a similar vein, Forensic techniques are introduced in the Incident Response process by NIST (2012). The economic value of these activities is not only in terms of prosecution, but could also help to reduce uncertainty, enhance recovery, loss estimation and help with the deterrence.

The literature thus points to three mechanisms which are interrelated. Initially, cybercrime might cause a welfare loss on the demand side due to loss of trust, heightened fear and diminished digital engagement. Second, it can have supply-side welfare effects in terms of the cost of cybersecurity investments, incident-response costs, recovery costs and reputational damage costs. Third, the application of cyber security and digital-forensic capabilities could affect the extent of the loss prevention, identification, containment and recovery.

Despite these understandings, there are still a number of issues which cause the literature to be divided into categories of cybersecurity economics, digital trust, welfare economics and digital forensics. While there are significant studies on the cost of cybercrime, the cost of security investments, consumer and producer surplus, contraction of digital transactions, dead weight loss and social welfare, the relationship of these to cybercrime has received comparatively little conceptual attention. This is the heart of the theoretical gap which is the present study tries to fill.



Therefore, the following section elaborates an integrated conceptual framework, where cybercrime is considered not just a security or criminal-justice issue, but also as a possible source of market distortion and loss of welfare in the digital economy.

### 3. Methodology

The supply side effects of cyber-crime contribute to the demand side effects with regard to trust. There are several ways in which organisations respond to cyber risk, such as cybersecurity investment, monitoring, compliance, incident response, insurance, recovery and technological upgrading. Gordon and Loeb (2002) describe information-security investment as an economic choice between the loss and the allocation of resources, and Anderson et al. (2019) illustrate how cybercrime has an impact beyond the immediate victim that causes social and economic damages.

Even if an organisation manages to keep a big breach at bay, these costs can still decrease producer surplus. Security, compliance and monitoring and preparedness for incidents have an opportunity cost relative to other activities that could be done with that resource, such as production, innovation, marketing or expansion of service offerings. Other expenses can be incurred after an incident such as investigation, system restoration, customer compensations, legal proceedings and reputation damage. So cybercrime can impact producer welfare both in terms of actual losses, and in terms of the resources needed to deal with cyber risk.

Digital forensics takes this relationship to a whole new level. Digital forensic processes are used to facilitate the identification, preservation, examination and interpretation of digital evidence, and can help with incident reconstruction, attribution, loss assessment, and legal matters (Casey, 2011; Carrier, 2005). In a similar vein, Forensic techniques are introduced in the Incident Response process by NIST (2012). The economic value of these activities is not only in terms of prosecution, but could also help to reduce uncertainty, enhance recovery, loss estimation and help with the deterrence.

The literature thus points to three mechanisms which are interrelated. Initially, cybercrime might cause a welfare loss on the demand side due to loss of trust, heightened fear and diminished digital engagement. Second, it can have supply-side welfare effects in terms of the cost of cybersecurity investments, incident-response costs, recovery costs and reputational damage costs. Third, the application of cyber security and digital-forensic capabilities could affect the extent of the loss prevention, identification, containment and recovery.

Despite these understandings, there are still a number of issues which cause the literature to be divided into categories of cybersecurity economics, digital trust, welfare economics and digital forensics. While there are significant studies on the cost of cybercrime, the cost of security investments, consumer and producer surplus, contraction of digital transactions, dead weight loss and social welfare, the relationship of these to cybercrime has received comparatively little conceptual attention. This is the heart of the theoretical gap which is the present study tries to fill.

Therefore, the following section elaborates an integrated conceptual framework, where cybercrime is considered not just a security or criminal-justice issue, but also as a possible



source of market distortion and loss of welfare in the digital economy.

#### 4. Results

This proposed welfare economics framework shows that cybercrime has a negative impact on the digital market's efficiency and efficiency cannot be ignored. In a conceptual model (Figure 1), cybercrime is a negative externality that has a negative impact on the demand and supply side of the digital markets. Demand-side effects of cyber incidents like phishing, identity theft, online booking fraud, and social media scams include decreased consumer confidence in transactions, enhanced transaction risks, and consumer reluctance to engage in digital commerce. This decrease in digital transactions therefore has an impact on consumer surplus, because consumers miss out on mutually beneficial trades because of increased uncertainty and security worries.

On the demand side, cost of doing business is rising for organisations regarding cyber security infrastructure, incident response, regulatory compliance, cyber insurance, litigation and reputation recovery. Such costs raise the real cost to the provider of digital services, and lower producer surplus. The more investments go into defending against attacks, the less goes towards generating new business. The more the firms spend on defense, the less on creation of new businesses.

A decreasing consumer confidence and rising producer costs reduces the amount of equilibrium output of digital transactions, causing dead weight loss. This welfare loss is the value of transactions when cybercrime is not present but the value is lost due to increased risks and also higher transaction costs. As such, the more limited economic impact of cybercrime, as measured by financial damages, is a miscalculation.

The framework also proposes that there are distinct welfare impacts of the different types of cybercrime. The main impact of financially motivated crime on consumer surplus occurs through monetary losses, and loss of consumer confidence in electronic transactions; phishing and digital payment fraud are the most common types of these types of crimes. Ransomware and large-scale data breaches, on the other hand, can cause significant producer surpluses to be lost due to disruptions to operations, recovery costs, and reputational damage. Social engineering attacks, cyber grooming and social media fraud engender more general social welfare losses due to diminishing and impacting digital trust and its potential long-term users.

These relationships lead to some conceptual propositions. Proposition 1: The more intense cybercrime is, the lower consumer surplus will be due to lower trust and higher perceived transaction risk. Proposition 2 states that as a result of cybercrime, producers' operating costs rise, leading to a decline in producer surplus and organisational competitiveness. In digital markets, Proposition 3 suggests that the loss of consumer surplus and producer surplus give rise to measurable deadweight loss which translates into lower total social welfare in digital markets.

Together these results situate cybercrime as a market failure that is beyond technical vulnerability and law enforcement issues. The proposed framework is a theoretical framework to merge the concepts of welfare economics and cybersecurity/digital forensics for future



empirical studies to measure the hidden costs and consequences of cybercrime with indicators like consumer trust, cybersecurity investments, digital transactions, forensic evidence etc. generated from cyber incident investigations.

## **5. Discussion**

The proposed welfare economics model adds to the existing economics of cybercrime literature by showing that the impact of cybercrime can't be fully captured by merely the financial losses or the cost of cybersecurity investment. Previous research has tended to focus on the economic motivations of cybercriminals (Moore, Clayton, & Anderson, 2009); optimal investment in cybersecurity (Gordon & Loeb, 2002); and the cost of cyber incidents to an organisation (Romanosky, 2016). Although these and other contributions have taken a big step forward in the economics of information security, they do not give much insight into how cybercrime affects market efficiency and the welfare of society.

The results of this research highlight the thesis of cybercrime as an information asymmetry type of market failure with negative external effects and higher transaction costs. This interpretation is in line with Akerlof (1970), who suggested that uncertainty about the security of transactions deters mutually beneficial transactions. Likewise, the decrease in digital participation in the proposed framework is consistent with Stigler's (1961) claim that imperfect information raises search and transaction costs and lowers market efficiency. This loss of consumer confidence further strengthens the need for trust in E-commerce, which was shown to be an essential determinant of online purchase by Gefen, Karahanna and Straub (2003) and Pavlou (2003).

Theoretically, the present study builds on the classical theories of Marshall (1890) and Pigou (1920) by introducing cybercrime as a negative externality which not only causes a decrease in the consumer's surplus but also a decrease in the producer's surplus and a deadweight loss in the digital market. The proposed framework is different from previous cybercrime studies which mainly focused on quantifying directly observable financial damages and include welfare losses associated with missed opportunities for economic engagement, reputation damages and organisational security expenditures. The paper thus introduces a novel interdisciplinary approach in which the concepts of welfare economics, cybersecurity and digital forensics are combined in a single analytical framework. This integration will help policymakers, businesses and researchers to gain a wider picture of the societal impact of cybercrime and guide the empirical research needed to quantify the welfare cost of cybercrime in the digital economy in the future.

## **6. Limitations and Future Research**

There are several limitations for this study. First, the proposed framework is conceptual and has yet to be tested using empirical data from primary or secondary sources. There is therefore a theoretical basis only between the concepts of Cybercrime and the notions of consumer surplus, producer surplus and deadweight loss. Second, the framework lacks a distinction between the welfare impacts of different types of cybercrime and the different types



of digital markets within a given sector, whose effects can be different. Thirdly, the study uses a static welfare framework and hence fails to reflect the time series development of cyber threats, consumer trust and organisational resilience.

The proposed framework should be empirically tested either by adopting multi-source secondary data (cybercrime statistics, digital payment fraud data, consumer trust surveys, and cybersecurity expenditure of organisations) or by conducting a survey of these figures. Prominent methods for determining the main drivers of welfare loss are advanced analytical methods like the Structural Equation Modelling (SEM), panel data regression (PANDA), System Dynamics modelling and Multi-Criteria Decision-Making (MCDM) approaches, such as the Analytical Hierarchy Process–TOPSIS (AHP–TOPSIS), and the Delphi (DEMATEL). Besides, future research could create a Cybercrime Welfare Loss Index (CWLI) to measure industry and country level loss of consumer surplus, producer surplus, and deadweight losses to help policymakers better estimate the socioeconomic consequences of cybercrime and target cybersecurity spending accordingly.

## 7. Conclusion

Cybercrime has been traditionally studied technologically, legally and financially, with only limited research and consideration of the economic welfare implications of cybercrime. In this paper, the author fills that void by designing a new welfare economics concept of cybercrime as a market failure that creates a loss of consumer surplus, producer surplus, and total social welfare, through a deadweight loss. The paper combines the fields of welfare economics, cybersecurity and digital forensics to present a holistic theoretical framework to comprehend the indirect welfare economic effects of cybercrime, in addition to the direct financial costs. The proposed framework supports the developing economics of cybersecurity by laying the groundwork for empirical studies in the future and can serve as a basis for evidence-based policy decisions, cybersecurity investments by organisations, and the regulation of digital markets. Finally, to treat cybercrime as an externality that reduces welfare highlights the importance of collective action between governments, businesses and consumers to create resilient, trusted and sustainable digital ecosystems.

## References

- Acquisti, A., Taylor, C., & Wagman, L. (2016). *The Economics of Privacy*. Journal of Economic
- Akerlof, G. A. (1970). *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*. Quarterly Journal of Economics
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). *Measuring the Cost of Cybercrime*.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). *Insurability of Cyber Risk: An Empirical Analysis*. The Geneva Papers on Risk and Insurance.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). *Trust and TAM in Online Shopping*. MIS Quarterly



Gordon, L. A., & Loeb, M. P. (2002). *The Economics of Information Security Investment*. ACM Transactions on Information and System Security.

Marshall, A. (1890). *Principles of Economics*

Moore, T., Clayton, R., & Anderson, R. (2009). *The Economics of Online Crime*. Journal of Economic Perspectives.

Pavlou, P. A. (2003). *Consumer Acceptance of Electronic Commerce*. International Journal of Electronic Commerce.

Pigou, A. C. (1920). *The Economics of Welfare*

Romanosky, S. (2016). *Examining the Costs and Causes of Cyber Incidents*. Journal of Cybersecurity .

Stigler, G. J. (1961). *The Economics of Information*. Journal of Political Economy .