

Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Preventing Pirated Software Use within an Organization

CAPSTONE REPORT

Jared A. Corwin
Sr. System Administrator
All Net Connections

University of Oregon
Applied Information
Management
Program

Spring 2018

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

Dr. Kara McFall
Director, AIM Program

Preventing Pirated Software Use within an Organization

Jared Corwin

All Net Connections

Abstract

Software piracy, or the illegal use of software, is a growing global issue. The legal and moral ramifications associated with the use of pirated materials within an organization increase the risk of criminal and civil liabilities within an Information Technology (IT) department. This study examines select literature to discover what can and should be done by an IT worker to prevent the use of pirated materials on the network for which they are responsible.

Keywords: software piracy, digital piracy, information technology, copyright infringement, pirated media, distribution companies

Table of Contents

Abstract	3
Introduction to the Annotated Bibliography	7
Problem	7
Purpose.....	9
Research Question	9
Audience	10
Search Report.....	10
Keywords.....	11
Search engines and databases.....	11
Documentation approach.....	12
Reference evaluation criteria	12
Annotated Bibliography.....	14
Background and Information on Digital Piracy	14
Piracy Prevention Methods.....	22
Ethics and Psychology of Software Piracy	30
Conclusion	41
References.....	46

Introduction to the Annotated Bibliography

Problem

In 2008, Chiu, Hsieh, and Wang (2008) identified software piracy as the greatest issue facing the modern software industry. Software piracy is defined as “the unauthorized copying of an organization’s internally developed software or illegal duplication of commercially available software to avoid fees” (Wagner & Sanders, 2001, p. 163). Craig and Burnett (2005) note “Piracy is robbery, an infringement of a copyright” (p. 3).

Software was not recognized as intellectual property until the Computer Software Copyright Act of 1980, which enabled compiled applications to be copyrighted (Craig & Burnett, 2005). In 1989, the United States Patent Office began to award patents to software developers, thus assigning the rights to the compiled programs and underlying source code to the software developers (Craig & Burnett, 2005). With the passage of the No Electronic Theft (NET) Act into law in 1997, the definition of “commercial advantage or private financial gain” was amended to include the exchange of copies of copyrighted works, regardless of whether money was paid for the copies (Craig & Burnett, 2005, p. 187). Persons who violate the NET Act are committing a felony and are subject to up to five years in prison and \$250,000 in fines (Craig & Burnett, 2005); civil penalties of up to \$150,000 can be assessed for every instance of an illegal copy of software (Bailey & Soileau, 2011). Currently, software piracy is a federal offense and considered to be organized crime (Craig & Burnett, 2005).

The Business Software Alliance (BSA) was established in 1988 as an anti-piracy alliance that now has members from 65 countries who represent some of the world’s largest software manufacturers (Craig & Barnett, 2005). Globally, the BSA reported in 2016 that 39% of computers had pirated software installed on them (Wu, Nan, & Li, 2018). In the same 2016

report, the BSA noted that 26% of workers loaded unauthorized software onto company networks, a figure that was nearly double the estimate of many CIOs (Wu, Nan, & Li, 2018). “Even in certain critical industries, including banking, insurance and securities, the unlicensed use rate worldwide amounts to 25%” (Wu, Nan & Li, 2018, p. 219).

Software piracy is a detriment to a firm’s profits, as the sales of legal software decrease in turn (Gomes, Cerqueira, & Almeida, 2015). The commercial value of pirated software in 2010 was \$58.8 billion, a figure that rose to \$63.4 billion in 2011 (Han et al., 2014). The BSA reports losses due to software piracy annually (Gomes, Cerqueira, & Almeida, 2015), and in 2014 reported that a 1% increase in software licenses sold benefits the economy by \$73 billion, whereas a 1% increase in pirated software only benefits the economy by \$20 billion (Han et al., 2014). This discrepancy points to the larger impact piracy can have above and beyond just hurting a corporation’s bottom line (Han et al., 2014).

Beyond the legal and financial consequences that can result from using pirated software is the issue that many of the sites one visits to obtain pirated software often harbor more instances of computer viruses and spyware than most other sites (Craig & Burnett, 2005). The tools necessary to circumvent copyright protections on pirated software are known as either cracks or keygens and these tools are usually bundled with the pirated software when it is downloaded (Kammerstetter, Platzer & Wondracek, 2012). A study performed by Kammerstetter, Platzer and Wondracek (2012) found that “the chance of being exposed to malicious code when dealing with cracked applications or games is more than 50 percent” (p. 818). The BSA found similar results in their 2016 report, noting “the higher the rate of unlicensed PC software, the higher the likelihood that users will experience potentially debilitating malware” (BSA, 2016, p. 4).

In 2015, \$400 billion was spent responding to cyberattacks globally, and the average estimated cost of an attack on an organization is \$11 million (BSA, 2016). The U.S. Council of Economic Advisors (2018) issued a report in February 2018 that pegged the cost of cyberattacks to the U.S. economy in 2016 as between \$57 billion and \$109 billion. The report further noted that businesses are often linked electronically to other businesses, and thus the damage of a cyberattack against one firm actually results in magnified damage to the economy (Council of Economic Advisors, 2018). The cost of cyberattacks against a large firm is not only measured by the cost to restore systems and lost revenue; large firms in 2016 that experienced an attack lost on average 0.8 percent of their stock market value in the seven days following news of the attack (Council of Economic Advisors, 2018). Pirated software that exposes users and their employer to malware contributes to an issue that represents a significant domestic economic threat (BSA, 2016; Council of Economic Advisors, 2018).

Purpose

The purpose of this study is to examine select literature to identify best practices for Information Technology (IT) personnel seeking to prevent the use of pirated software within their organizations. The study is framed for IT workers, IT management, Chief Information Officers (CIOs) and IT committee members and aims to foster a strategic, systematic and cooperative approach to protect against piracy.

Research Question

What are best practices for IT department personnel seeking to prevent the use of pirated software within their organizations?

Audience

This study is designed to be beneficial to IT workers, IT management, Chief Information Officers (CIOs) and IT committee members, all of whom are impacted by pirated software within their organizations. Regardless of the environment in which the IT professionals work, it is important to protect the network, the organization and themselves from the dangers and legal implications of pirated software operating within a production environment. Information Technology workers and managers alike may be unaware of the existence, prevalence and consequences of pirated software, may not know the ethical response if such software is found, and may be unaware of the best practices for prevention. CIOs and IT committee members will be charged with allocating resources to enable the tools and processes to prevent pirated software from appearing on their networks. This study will provide information from the literature on procedures that can be implemented immediately to successfully reduce, if not fully eliminate, pirated software.

Search Report

Search strategy. I used the University of Oregon Libraries' database search engine to identify scholarly articles. I chose keywords based upon the generally known terms connected to my subject matter. In this case, I used words like *software* and *piracy* to narrow the results to those related to the research problem. Searching with these terms resulted in a large number of results; it was necessary to narrow the returned items to sources more specific to the research topic.

I filtered the results by first choosing to only receive results from academic journal articles. This resulted in another large selection of items, so I added a filter that limited search

results between the years of 2007 and the current date. This resulted in a manageable number of results that could be skimmed and noted for further investigation.

Keywords. I used various keywords both individually and in combination to find more specific articles. The keywords I used were the following:

- Software piracy.
- Digital piracy.
- Information technology.
- Information systems.
- Copyright infringement.
- Pirated media.
- Distribution companies.
- Media content creators.
- BASCAP (Business Action to Stop Counterfeiting and Piracy).
- Why companies pirate software.
- Factors motivating software piracy.

Search engines and databases. I used Google's search engine to find the meaning or names of acronyms and certain terms used in other academic articles. The main tool I utilized in searching for articles was the University of Oregon Libraries OneSearch. On occasion, the selection of an article took me to the website of a specific database where I utilized the specific database search engine to find new materials. The databases I utilized from the University of Oregon Libraries are the following:

- Academic OneFile.
- Business Source Complete.

- JSTOR.
- Science Direct.
- ProQuest.
- Factiva.
- Sage Journals.

Documentation approach. Zotero is the tool that I used to track and record my references. I saved a copy of every referenced item locally to a OneDrive folder for backup to the cloud. After saving a source in OneDrive I copied the article to Zotero via drag-and-drop. Zotero creates a full APA-formatted reference for further use, although it was necessary to manually check the references as the tool produced some errors.

I created a Microsoft Word document that is also backed up to my online OneDrive account to document search strategies and keywords. Every time I performed a search I logged which search engine was used and all of the keywords used to perform the search. I recorded any articles that I found during a search on the same document by adding the author's name and the abstract or URL. Documenting the information in this fashion allowed me to capture the searches I used to locate each article; I then used this data to further filter results that were more closely related to the chosen subject areas.

Reference evaluation criteria. I evaluated references utilized for the purposes of this study using the criteria provided from the Center for Public Issues in Education (n.d.). The five criteria are: *authority*, *timeliness*, *quality*, *relevancy* and lack of *bias*. Materials were considered authoritative if they came from reputable publishers or organizations and peer-reviewed journals. Much of the data that is collected on piracy is collected by organizations that have a bias to some extent, as they are generally fighting against the growth of piracy. I considered the bias of each

source carefully, and judged for bias based upon the document's cited use in various peer-reviewed journal articles, as these documents have gone through a rigorous review and editing process. Sources that were published by vendors selling related products or services were rejected due to clear bias concerns.

The topic of digital piracy is relatively recent; therefore, I selected sources written no earlier than 2007. The data within the articles includes information collected from 1999 to 2016. I ensured the quality of references by limiting my selection of sources to those that utilized proper grammar, punctuation and spelling. I carefully considered the relevancy of each reference after a thorough review of the material and a judgment as to the appropriateness of the content to the subject matter in this study.

Annotated Bibliography

Introduction to the Annotated Bibliography

The following annotated bibliography presents 15 references that explore the socio-economic factors that are either influenced by or the result of the act of software piracy globally. References were selected to discover the means and motivations behind those that pirate software and in doing so provide necessary information for IT professionals to address the issue within their organizations. References are presented in three categories that provide context for and a thorough understanding of the issue: (a) background and information on digital piracy; (b) piracy prevention methods; and (c) ethics and psychology of software piracy.

Each annotation consists of three elements: (a) the bibliographic citation, (b) an abstract, and (c) a summary. For works that include a published abstract, the abstracts are presented complete as published. All other abstracts were written by the author of this annotated bibliography based upon my understanding of the material. The summaries were written to relate the article's information to one of the three reference categories that serve to provide information to address the problem statement of this study. The information collected may serve to assist IT professionals in understanding the problem of software piracy and in reducing the risks associated with a lack of awareness of the issue.

Background and Information on Digital Piracy

Brown, S. C. (2014). Approaches to digital piracy research: A call for innovation. *Convergence:*

The International Journal of Research into New Media Technologies, 20(2), 129–139.

<https://doi.org/10.1177/1354856513517470>

Abstract: With its focus on the field of digital piracy (DP), the February 2013 special issue of *Convergence* explored a number of novel research topics using unconventional research methods. In doing so, the issue stands out from the bulk of DP research, which often concentrates on economic and commercial aspects. Such concerns demand particular research methods that are in turn subject to limitations. Drawing from a broad range of literature across various disciplines, this article both explores these limitations and demonstrates that alternative approaches exist, which can greatly enhance the understanding of digital piracy on a more holistic level. The article concludes with suggestions for future research, arguing in particular that cross-discipline research will best serve the field by promoting innovative methods of data collection and analysis.

Summary: This article provides an analysis of various literature concerning the act of digital piracy (DP) and how much of the available research is limited or based upon limited data sets. Importantly, the author marks the distinction in the multiple types of piracy that exist and notes that the generalization of the term *piracy* lends itself to inaccurate conclusions by not differentiating the types of piracy that are being studied. The author advocates that research on digital piracy be broken into categories based upon the type of digital media: music, movies, and software. He notes that people seek out different types of digital media for different reasons; thus, research on digital piracy should also be differentiated based upon media type.

The author illustrates the limitations of quantitative research studies that have utilized economic, criminal and self-disclosure models of analysis and offers alternative approaches that would provide informative qualitative data to better understand the concept of DP. Limitations of past qualitative studies noted by the author include the

overreliance on the use of college students in self-reported studies and the use of crude scales to measure downloads by a user. The author recommends including a wide sample of adults in self-reporting studies to gain a more accurate data set and asking specific questions relating to pirated downloads to address the shortfalls of past studies.

The author also notes distinctions between those who pirate to sell the pirated material for profit and those who pirate for other reasons, including not wanting to pay for the material or negative social stigmas from the pirating community at large. Key distinctions between the two groups who pirate are the motivations that cause them to pirate: making a profit or for fun.

This article is relevant to this study because it offers background information and a basic understanding of the concept of digital piracy and the flaws in past research in this area.

Craig, P., & Burnett, M. (2005). *Software piracy exposed*. Rockland, MA: Syngress Publishing, Inc.

Abstract: This book dives into the unique world of software piracy. It explores the personalities and motivations of those behind much of the illegal software distribution on the Internet. Paul's aggressive investigation and reporting of this world allowed him to explore the inner depths of the software piracy scene and gained him exclusive interviews with some of the most notorious individuals in the scene. Throughout the course of his year-long investigation, Paul sought out the individuals behind this highly organized collection of individuals who somehow flew under most of the public's radar. Everyone seems to know about P2P networks, but few are familiar with top sites, couriers, and other aspects of the software piracy scene.

Summary: This book offers an in-depth look at the historical and current piracy of digital media and why those who choose to pirate do so. Historically, the author notes that pirating software consisted of making copies of a physical medium and distributing the copies with the license key so that the software could be installed on multiple different systems. However, as the internet has evolved, the author describes groups that have arisen that exist solely to crack or break the software protections of various types of software and distribute the software over the internet. The author shares that it takes only twelve days on average after software is released before it has been cracked and shared on the internet.

The author details the laws for digital piracy and how they have evolved to meet the new technologies and methods that are being used to crack or distribute pirated materials.

Originally, the author notes that laws governing digital piracy were lacking as software was treated as intellectual property and thus there were no laws against reproducing the material. Today, the author states that laws have evolved to consider software piracy as organized crime and notes that those sentenced with this crime have no chance of parole.

The author concludes that copyright protections will need to evolve as current attempts have done little to deter the growing rates of piracy.

This source is relevant to this study because it offers a history of how software has been pirated and the reasons why, as well as providing the historical context surrounding the legal battles over digital piracy.

Gomes, N. D., Cerqueira, P. A., Almeida, L. A. (2015). A survey on software piracy empirical literature: Stylized facts and theory. *Information Economics and Policy*, 32, 29-37.

<http://linkinghub.elsevier.com/retrieve/pii/S0167624515000293>

Abstract: As software is central in today's world, the problem of software piracy is of increasing importance. It reduces the revenues of firms that develop new software and, therefore, it may hinder innovation and growth. To understand better the causes of this phenomenon this paper presents a survey of the empirical literature regarding software piracy and discusses if the findings are coherent with the theoretical literature. Overall we are able to identify eight stylized facts in five dimensions: the Economic, Cultural, Educational, Technological and Legal. Moreover, we argue that most of these findings are coherent with that which the theoretical models imply.

Summary: The authors aim to understand ways in which to prevent software piracy by conducting a survey of the empirical literature related to software piracy. The authors utilized a five-category classification system (economic, cultural, educational, technological, and legal) to analyze software piracy literature. Key findings include that empirical study results tend to show that educated individuals who are aware of the long-run costs of pirating such as legal ramifications and fines or those who require certain quality thresholds in their software tend to be less likely to pirate, even if they have the knowledge to do so. Another finding relates the gross domestic product (GDP) per capita to lower levels of software piracy; the authors found that residents of countries with lower GDPs were more likely to pirate.

The authors' main concern in their study was the possibility of biases in some of the data sources used by a subset of the literature sources they analyzed. The authors were

concerned about implicit bias because the data was procured from the Business Software Alliance, a group that represents companies and therefore is not a completely unbiased source of information. The authors assert that future research studies should acquire data from different sources.

This source is relevant for this study because it examines the categorical root causes of software piracy. The article also offers evidence of how educational systems can have a positive effect on decreasing the use of pirated software and highlights the fact that technological and legal frameworks meant to deter piracy need to be better understood.

Nil, A., Shultz, C. J. (2009). Global software piracy: Trends and strategic considerations.

Business Horizons, 52(3), 289-298.

<http://linkinghub.elsevier.com/retrieve/pii/S000768130900024X>

Abstract: The design, manufacture, distribution, and sale of software constitutes a rapidly growing and remarkably lucrative global industry. Leaders of most software companies understand that intellectual property rights (IPR) typically are vital to competitive advantage and company success. Theft of intellectual property (IP) in the form of software piracy is brazen, extremely costly, lowers incentives to innovate, and threatens the very existence of some companies. IP theft, therefore, is a daunting challenge for managers of software firms. In this article, we make several contributions that should prove helpful to software designers, managers, responsible users, and broad stakeholders of software innovation and use—that is, almost all of us. In doing so, we provide an overview of international legal, ethical, economic, and systemic considerations, and we share an analysis of the drivers of consumer software piracy. We

then discuss strategic considerations and introduce a decision-making typology, which may help legitimate companies to devise strategies and tactics to manage their software IP in the face of widespread piracy.

Summary: This article analyzes the global threat of piracy through the use of a typology based upon two key factors: strategic importance of the intellectual property (IP) and the likelihood of infringement. Though the authors' focus is to offer suggestions to software developers on ways to prevent their materials from being pirated, the authors present information on leading factors that influence global piracy of protected materials. The authors note that awareness of strict laws and tough enforcement, like those in the United States, serve as deterrents to piracy. They identify consumers who are younger, computer literate and tech savvy – traits that are found in many employees of IT departments – as the most likely to commit software piracy. The authors recommend that the focus of education and training to discourage software piracy be applied to the above demographic to have the best impact. The authors also found that one of the most important factors influencing those who pirate software is the affordability of the software; the more expensive the software, the more likely it will be pirated.

This article is relevant to this study because it describes the drivers of software piracy and provides information about the consumers who are most likely to engage in software piracy.

Panethiere, D. (2005). The persistence of piracy: The consequences for creativity, for culture, and for sustainable development. *The Global Alliance for Cultural Diversity, United*

Nations Educational, Scientific and Cultural Organisation (UNESCO).

<http://unesdoc.unesco.org/images/0014/001455/145517e.pdf>

Abstract: Note: Abstract provided by the author of this annotated bibliography in the absence of a published abstract. This study on piracy was prepared at the request of the Cultural Enterprise and Copyright Section as part of the anti-piracy program established under the framework of the Global Alliance for Cultural Diversity project at UNESCO. The author defines piracy in the context of the internet and explains how it has evolved over time. The general theme of piracy is broken down into the component Medias that are commonly pirated and an explanation and data are provided for each component. The author notes the negative effects that piracy has on culture, developing countries and creative industries. Finally, a section is offered that explains the multiple means that are being used to combat piracy and the results in terms of those that are successfully making an impact and those that are not.

Summary: This study was requested by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) to provide data on the effects of piracy in the areas of creativity, culture and sustainable development. The study covers many different types of digital media that is pirated including music, movies, software, books, and television. In regards to software piracy, the author claims that in 2003 29 billion USD worth of software was pirated and installed globally. The author found the scale of piracy to be large at the time of the study, reporting piracy rates around the world in 2004 as:

1. US – 23%.
2. Western Europe – 36%.
3. Asia/Pacific – 53%.
4. Eastern Europe – 70%.

5. Latin America – 63%.
6. Middle East and Africa – 55%.

The author suggests that a great deal of training and instruction in best practices are needed before any real improvement will occur in the rate of piracy worldwide. This bulletin is relevant to this study because it provides data on the consequences and scale of software piracy globally.

Wu, D., Nan, G., Li, M. (2018) Optimal software upgrade strategy: Should we sell products or premium services in the presence of piracy? *Electronic Commerce Research and Applications*, 28, 219-229.

<http://linkinghub.elsevier.com/retrieve/pii/S156742231830022X>

Abstract: This research explores the software upgrade strategy in the presence of piracy. When a firm introduces an upgrade, it can adopt a freemium strategy, by offering free products and paid services, or by adopting traditional strategy, and continuing to sell products. We develop a two-period joint model of upgrading and piracy, and use it to compare these two strategies. We find that whether a firm should adopt copyright protection depends on the reservation price for unethical consumers. Additionally, the presence of piracy and premium services can reduce price competition between the original product and the improved version. Freemium strategy always dominates traditional strategy except when the two conditions are satisfied. First, the differentiation between the original product and the improved version in terms of consumer preference must be relatively small. Second, the differentiation between the original product and the improved version in terms of product value must be moderate.

Summary: The aim of the authors was to investigate whether a firm can discourage software piracy by selling upgraded versions of a product rather than giving away a base

product for free and charging for premium add-ons. The authors utilized a two-period economic model to determine if a firm should sell products or premium services or adopt the *freemium* strategy of offering the base product for free and charging for add-ons. Their results show that the freemium strategy increases the firm's market share when compared to releasing an updated version of a product that is sold rather than given away. The authors also found that a firm should not try to protect the software with copyright protection when the reservation price for unethical consumers, or those willing to engage in piracy, is relatively low. Not securing copyright protection for the software in the presence of piracy can reduce price competition, allowing for the higher price for the legally obtained version of the software. This article is relevant to this study because it presents relevant data that is current within the last few years on potential software pricing and copyright protection strategies to thwart piracy.

Piracy Prevention Methods

Chiu, H.-C., Hsieh, Y.-C., & Wang, M.-C. (2008). How to encourage customers to use legal software. *Journal of Business Ethics*, 80(3), 583–595. <https://doi.org/10.1007/s10551-007-9456-7>

Abstract: This study attempts to identify customer retention strategies for legal software and discusses their effectiveness for three consumer groups (stayers, dissatisfied switchers, and satisfied switchers). Although previous studies propose several antipirating strategies, they do not discuss how to enhance customer intentions to use legal software, which is crucial for software companies. The authors provide four generic retention strategies developed from both antipiracy and customer loyalty literature. The results indicate lower-pricing, legal, communication, and product strategies all enhance

customer purchase intentions toward legal software. The lower-pricing strategy is more useful for stayers and dissatisfied switchers, and the communication strategy is most useful for dissatisfied switchers. Both the legal and product strategies have similar impacts on purchase intentions across the three segments. From a firm perspective, a product strategy is most worthwhile and useful across all segments.

Summary: The aim of this study is to provide customer retention strategies to software development companies and then test their effectiveness. The authors developed four generic strategies from literature to improve customer loyalty and the effectiveness of antipiracy efforts. The authors first divided software users into three different categories: dissatisfied switchers, satisfied switchers and stayers. Dissatisfied switchers are users of pirated software who are not satisfied with the quality of the pirated software, and so switch to a legal version. Satisfied switchers switch from pirated software to legal software for reasons other than quality. Stayers only use legal software and therefore do not switch at all.

The authors found that the implementation of customer loyalty strategies with antipiracy strategies were important in increasing the use of legal software. The strategies that represented desire-based determinants were lower pricing and communication strategies. Communication strategies included releasing information to the public about the risks that are associated with software piracy as well as the benefits of using legal software. The legal strategy was considered a constraint-based determinant. The product strategy included both constraint-based and desire-based determinants by providing both benefits of using the software legally and barriers to piracy. The product-based strategy was found to be the most beneficial across the three targeted groups.

The authors note two main concerns in this study. The first is that the data pool consisted of people only in Taiwan, and so the results may suffer from external validity. Second, the authors limited their strategies to software firms only, and so generalizing their conclusions to other industries may not be accurate.

This article is relevant to this study because it provides information on strategies to deter software piracy. Though the authors' focus is from the perspective of software development companies, the results are insightful and can be used when forming a more general policy on software piracy.

Djekic, P., & Loebbecke, C. (2007). Preventing application software piracy: An empirical investigation of technical copy protections. *The Journal of Strategic Information Systems*, 16(2), 173–186. <https://doi.org/10.1016/j.jsis.2007.05.005>

Abstract: To counteract application software piracy, software publishers have been implementing preventive technical copy protections into their software products. However, scientific research has not yet empirically investigated to what extent technical copy protections avoid illegal copying. Investigating this question, the paper studies the influence of technical copy protections on application software piracy. We apply descriptive statistics and a binary logistic regression to data collected from a survey of international software users. We show that technical protections fail in protecting application software from being illegally copied; none of the measures studied significantly avoids piracy. From this, we firstly derive implications for software publishers and researchers and secondly suggest directions for future research.

Summary: This study is an empirical investigation into the efficacy of technical copy protections on software piracy. The authors used a survey to collect data from international users and applied descriptive statistics and a binary logistic regression to the results. Their analysis indicated that there were no statistically significant variables that were found to be deterrents for either software-based or hardware-based protections. The authors did find that variables such as higher personal annual income, stronger software auditing requirements for the workplace, and stronger intensity of application software usage – a heavy reliance upon both the software and reliable support for the software – increased the likelihood of software being installed legally. The authors suggest that a strategy that is focused on deterrent controls like educational campaigns is better suited to stemming pirated software use over employing preventive controls such as web filtering and Digital Rights Management (DRM) protection software. The authors note limitations with their study in the use of an online survey that might have affected the quality of data due to the potential for conflicts stemming from self-incrimination concerns; they also note the corresponding likelihood of underreporting acts of piracy. This article is relevant to this study because it offers empirical evidence about the efficacy of specific types of pirating deterrents.

Han, Y., Choi, J., Cho, S., Yoo, H., Woo, J., Nah, Y., Park, M. (2014). A new detection scheme of software copyright infringement using software birthmark on Windows systems.

Computer Science and Information Systems, 11(3), 1055-1069.

<https://www.doiserbia.nb.rs/Article.aspx?ID=1820-02141400064H>

Abstract: As software is getting more valuable, unauthorized users or malicious programmers illegally copies and distributes copyrighted software over online service provider (OSP) and P2P networks. To detect, block, and remove pirated software (illegal programs) on OSP and P2P networks, this paper proposes a new filtering approach using software birthmark, which is unique characteristics of program and can be used to identify each program. Software birthmark typically includes constant values, library information, sequence of function calls, and call graphs, etc. We target Microsoft Windows applications and utilize the numbers and names of DLLs and APIs stored in a Windows executable file. Using that information and each cryptographic has value of the API sequence of programs, we construct software birthmark database. Whenever a program is uploaded or downloaded on OSP and P2P networks, we can identify the program by comparing software birthmark of the program with birthmarks in the database. It is possible to grasp to some extent whether software is an illegally copied one. The experiments show that the proposed software birthmark can effectively identify Windows applications. That is, our proposed technique can be employed to efficiently detect and block pirate programs on OSP and P2P networks.

Summary: This article details an experiment on the efficacy of the use of software birthmarks in identifying, blocking and removing pirated Windows applications in the context of uploads or downloads utilizing either online service provider (OSP) or peer-2-peer (P2P) networks. The authors define software birthmarks as unique characteristics of software programs that can be used to identify each program. They created a new type of birthmark based upon data within the dynamic link libraries (DLLs) and application programming interfaces (APIs) that are used in all Windows applications. The authors

developed an algorithm to create birthmarks of Windows applications that were stored within a database. Utilizing this database, the authors could then run a filtering program on all uploaded and downloaded applications and accurately determine if the application was from their birthmark database.

Their findings suggest that current birthmarks are limited by not being strong enough to prevent theft, by being too resource-intensive and thus counter-productive and that some birthmarks must be manually run by an executable to operate. The new birthmark they proposed was found to be capable of surpassing these limitations and working correctly. This article is relevant to this study because it provides data about current and proposed technologies to deter or prevent software piracy. In addition, the article provides information about the limitations of current technologies to protect software from piracy.

Jeong, B. K., Khouja, M. (2013). Analysis of the effectiveness of preventive and deterrent piracy control strategies: Agent-based modeling approach. *Computers in Human Behavior*, 29(6), 2744-2755. <http://linkinghub.elsevier.com/retrieve/pii/S0747563213002677>

Abstract: We use agent-based modeling approach to analyze the impact of various digital piracy control strategies on consumers, retailers, record labels, and artists. We model heterogeneous agent behavior, motives, and interactions to examine the consequences in terms of aggregate system behavior. Using a multi-agent programmable modeling environment (Netlogo), several experiments were conducted to test the simulation model and develop managerial insights. We show that an educational strategy is more effective when consumers are resistant to anti-piracy efforts and budgets for combating piracy are small. Furthermore, value-added service and low-price strategies

should be used to encourage legitimate purchases since legal and educational strategies alone deter piracy but do not provide consumers' incentives to purchase legitimate products. Therefore, effectiveness of piracy control strategies can be improved by combining a legal or an educational strategy with a value-added or a low-price strategy. We also find that the profit-maximizing strategies are different for different players in the supply chain. While the record label prefers a low-cost strategy, it is optimal for the whole supply chain to use combined legal or educational strategy with a value-added strategy. Therefore, there is potential for all parties in the supply chain being better off if the record label and the retailer cooperate in combating piracy.

Summary: The aim of the authors is to better understand how piracy control strategies impact consumer behavior. The authors used an agent-based model to analyze various piracy control strategies. Agent-based modeling is a simulation technique that can be applied to problems by defining sets of agents with related attributes, behaviors and performance-measuring functions. Once the agents were defined, the authors conducted multiple experiments to test their model and the hypothesis that different strategies of piracy control would have various impacts that were not uniform across industries affected by piracy. The authors considered four strategies: (a) legal strategy, or actions the music industry takes against pirates and antipiracy laws and regulations, (b) educational strategy, or the dissemination of information to consumers about the damage caused by piracy, (c) low-price strategy, or lowering the price to encourage buyers to purchase legal products rather than engaging in piracy, and (d) value-added service strategy, or providing added value or additional services to encourage buyers to purchase legal products.

Findings from these experiments suggest that there is no single strategy that will prevent software piracy. However, the authors found that an educational strategy is most effective at deterring piracy when the consumers are resistant and budgets for combatting piracy were small. The authors found that the most successful piracy control resulted from increasing both legal and educational strategies and offering a low-price strategy for the consumer.

This article is relevant to this study because it provides empirical data relating to how various strategies of piracy deterrence can be implemented to have a greater effect on reducing incidences of piracy.

Ethics and Psychology of Software Piracy

Cho, H., Chung, S., & Filippova, A. (2015). Perceptions of social norms surrounding digital piracy: The effect of social projection and communication exposure on injunctive and descriptive social norms. *Computers in Human Behavior*, *48*, 506–515.

<https://doi.org/10.1016/j.chb.2015.02.018>

Abstract: Using a national sample of 620 Internet users in the US, this study examined the extent to which social projection, communication exposure, and an interaction between the two, influenced individuals' perceptions about two subordinate types of social norms surrounding digital piracy: injunctive norms and descriptive norms. In line with the social projection model, individuals made social estimates about others' piracy attitudes and behaviors anchoring on their own personal attitudes and behavior. However, frequent communication exposure reduced the degree to which they relied on this egocentric thought process. In addition, the two-way interaction was contingent on

another condition (perceiver's own piracy behavior) indicating that communication exposure had differing implications for pirates and non-pirates. Theoretical and practical implications are discussed.

Summary: The authors aim to better understand how people generate their perceptions about social norms related to digital piracy. The authors implement theoretical frameworks based on: (a) the social projection model, which is a theoretical model that “suggests that people use a judgmental heuristic that allows them to make quick predictions about others anchoring on their own attitudes and behavior” (p. 507), (b) communication model of social norms, which consists of using “descriptive and injunctive norms which indicate perceptions of others' attitudes and behaviors” (p. 507), and (c) a focus theory of normative conduct, which states that “people are likely to engage in an action when they perceive it to be socially approved by many others and prevalent in society” (p. 507). Utilizing a 620-person sample, the authors empirically examine how social projection, communication exposure and interactions between the two influence perceptions about social norms in relation to digital piracy.

The main focus of the authors was to determine what effects the interactions between egocentric thought processes (social projections) and social learning (communication exposure) had on each other in the context of digital piracy and whether they competed with each other or reinforced one another. Previous studies only focused on social norms independently and not the interactions between the two differing norms. The results from this study suggest that social projection has an important role in the shaping of social norms and perceptions about software piracy. The authors also found that increasing the frequency of information communicated to a consumer decreased an individual's

tendency to anchor one's perceptions on their own personal views, and communication exposure works to slightly moderate perceived attitudes on digital piracy. Another finding suggested that it will be difficult to change the behavior of digital pirates as they tend to normalize their behavior through social projection, meaning individuals that already pirate software are more likely to interpret communication messages through their own egocentric view and that frequent exposure to anti-piracy messages will be normalized by the individual by rationalizing that an increased number of messages relates to a larger number of users engaging in pirating activities, thus justifying the behavior.

This study was limited by the use of the social projection model, which is known to be less accurate than other models. The authors suggest that future studies should examine more complex causal mechanisms and that they should employ a longitudinal approach or an experimental study.

This article is relevant to this study because it offers insights into the factors that motivate pirates' intentions and how understanding these intentions can lead to the creation of more effective strategies to deter digital piracy.

Culiberg, B., Kos Koklic, M., Vida, I., & Bajde, D. (2016). Examining the effects of utilities and involvement on intentions to engage in digital piracy. *Computers in Human Behavior*, *61*, 146–154. <https://doi.org/10.1016/j.chb.2016.03.029>

Abstract: Reflecting scholars' growing interest in the utilitarian aspects of consumer digital piracy, this research examines two types of utilities associated with obtaining digital files (i.e. the utility of downloading pirated files and of purchasing copyrighted

files) as factors driving consumer intentions to download pirated files. Moreover, we extend the findings of previous studies by including film/music involvement as a moderator between those utilities and intentions. The conceptual model was tested on a sample of 943 adult consumers. The results of our study confirm that the utility of purchasing copyrighted files has a negative influence on the intention to download pirated files, while the influence of the utility of downloading copyrighted files is positive. The moderating effect of film/music involvement was only found to be significant for the relationship between the utility of downloading pirated files and intentions. Based on these findings, implications for the affected industries are discussed, as well as future research opportunities.

Summary: This article provides an ethical examination of two different types of utilities associated with obtaining digital software: the utility of pirating the software and the utility of purchasing the software legally. The authors used a conceptual model to test a sample of 943 adult consumers. The authors hypothesized that in deciding between the two utilities, consumers would seek to maximize utility by choosing to act based upon the expected value of the return from the activity and the costs. The results from this analysis confirm the authors' hypothesis that one's expectation of benefits from obtaining pirated software were positively correlated to the likelihood of engaging in digital piracy. The authors also found that there was a reduction in pirating behavior if there were perceived benefits from purchasing software legally; that is, if there are channels available to purchase software legally that can provide value for the consumer, then the consumer will choose the legal option over engaging in digital piracy. The authors suggest that if software industry leaders want to decrease acts of digital piracy, they should look at the

specific benefits (speed, affordability, and collectability) that piracy-related channels offer and incorporate them into their own distribution channels.

This article was limited by a data pool that was collected from adults in a single country.

The authors note that due to differences in legal and regulatory frameworks there may be very different influences on the perceptions of pirating behavior among consumers in different countries.

This article is relevant to this study because it provides information directly relating to the reasons why a consumer chooses to obtain software legally or illegally and the consumer's motivations behind the choice.

Jackman, M., & Lorde, T. (2014). Why buy when we can pirate? The role of intentions and willingness to pay in predicting piracy behavior. *International Journal of Social Economics*, 41(9), 801–819. <https://doi.org/10.1108/IJSE-04-2013-0104>

Abstract: Purpose – Digital piracy is one of the most popular forms of intellectual property theft and is currently recognized as a crime in several countries. This begs the question, if persons are fully informed that digital file sharing is a crime and, if caught, can be legally prosecuted, why do individuals opt to engage in such criminal behavior? The purpose of the paper is to determine the psychological, social and economic factors influencing digital piracy. Understanding the social and psychological features of digital pirates is necessary if effected strategies are to be developed to deter the practice of digital piracy.

Summary: The aim of the authors was to determine psychological, social and economic factors that influence digital piracy behaviors. The authors built a model of behavior

developed by Triandis (1980) which explains individual's behavior in terms of "intentions, by what they think they should do, and by the consequences that they associate with a specific behavior" (p. 804). The data for this study was collected by surveys that were completed by citizens of Barbados. The authors found that a consumer's intentions and willingness-to-pay (WTP) both had the highest impact on the consumer's behavior. Intention was found to be the largest predictor of piracy behavior and the factors that had the largest impact on intention were attitudes, perceived consequences, relativism (feelings of guilt), education and facilitating conditions (ease of obtaining pirated materials). The factors that most impacted WTP were perceived importance, facilitating conditions, income and idealism.

The results imply that communicating messages that only speak to the consequences of digital piracy are limited in impact by not taking into consideration variables related to the environment, income, personal ethics, socio-psychological traits and education of consumers. The authors note that the study is limited by the 400 participants, all from one country, and may not be able to be generalized to a larger community.

This article is relevant to this study because it provides information about what factors impact the intentions of digital pirates and how those factors can be examined and incorporated into the creation of strategies to combat piracy.

Kos Koklic, M., Kukar-Kinney, M., & Vida, I. (2016). Three-level mechanism of consumer digital piracy: Development and cross-cultural validation. *Journal of Business Ethics*, 134(1), 15–27. <https://doi.org/10.1007/s10551-014-2075-1>

Abstract: Digital piracy as a continuing problem significantly impacts various stakeholders, including consumers, enterprises, and countries. This study develops a three-level mechanism of determinants of consumer digital piracy behavior, with personal risk as an individual factor, susceptibility to interpersonal influence as an interpersonal factor, and moral intensity as a broad societal factor. Further, it explores the role of rationalization and future piracy intent as outcomes of past piracy behaviors. The authors use survey data from four countries in the European Union to test the system of structural relationships. With an exception of the effect of consumers' susceptibility to interpersonal influence on piracy behavior, the conceptual model receives remarkably consistent support across the four countries. Specifically, perception of personal risk and moral intensity negatively affected the reported piracy behavior in all four countries. The results further support the negative influence of moral intensity and the positive influence of past digital piracy behavior on consumers' use of rationalization. Lastly, personal risk, rationalization, and past digital piracy behavior directly influenced consumers' intention to engage in digital piracy in the future. The study also discusses implications of the findings and identifies areas of future research.

Summary: The aim of this article is to understand social drivers of piracy and provide insights into the ways individuals rationalize their behavior in regards to digital piracy. The authors used data from a survey that spanned four European countries and then developed a conceptual model that explored three mechanisms of digital piracy behavior: (a) an individual-level mechanism reflected in perceptions of personal risk (direct consequences of engaging in digital piracy for a person), (b) an interpersonal-level mechanism reflected in a person's susceptibility to interpersonal influence (conformity to

reference group norms), and (c) a societal-level mechanism reflected in the concept of moral intensity (direct consequences of piracy behavior for the society). The results from the study show that perception of risk and moral intensity significantly and negatively impacted piracy behavior in all of the countries tested. Additionally, the findings offer empirical support for personal risk, rationalization, and past digital piracy behavior as significant indicators of the intent of a consumer to engage in digital piracy behaviors. The areas of personal risk and moral intensity were found to have the most significant impact on altering the intentions of a digital pirate. The authors suggest that communications meant to deter piracy should center on creating public awareness of personal and social consequences of piracy while also highlighting the negative impact this behavior has on the society at large.

This article is relevant to this study because it provides data on how to successfully alter the intentions of those engaged in piracy behaviors through the use of social drivers.

Limayem, M., Khalifa, M., & Chin, W. W. (2004). Factors motivating software piracy: A longitudinal study. *IEEE Transactions on Engineering Management*, 51(4), 414–425.
<https://doi.org/10.1109/TEM.2004.835087>

Abstract: The objective of this paper is to gain a better understanding of factors influencing software piracy. A model explaining the contribution of different factors to software piracy intention and its subsequent effect on actual software piracy is constructed based on established theories of human behavior. The model is then tested empirically in a longitudinal study with a survey. Findings show that social factors and beliefs concerning consequences of software piracy have significant effects on software

piracy intentions. The data also show that while habits and facilitating conditions were significantly related to actual piracy behavior, intentions did not necessarily lead to the actual act of software piracy. The implications of the findings to research and practice are discussed.

Summary: This article utilizes theories of human behavior to construct a model to explain factors that contribute to one's intentions to commit software piracy and the effects of those factors on actual software piracy. The authors test this model empirically by use of a longitudinal study including a survey. The authors chose to utilize the Triandis model to explain the behavior of individuals who commit software piracy in terms of habits, social norms, and perceived consequences/beliefs. The authors' findings indicate that social factors such as norms and values shared amongst friends or colleagues and perceived consequences can influence the intentions to pirate software. The authors assert that increasing awareness of the unethical nature of pirating software may not be enough to change attitudes towards piracy nor discourage piracy. The authors state that the most effective method found to decrease software piracy within an organization is for management to implement and enforce an ethical code and couple this with strong software copying policies that clearly state the criminal liabilities and penalties associated with this behavior.

This article is relevant to this study as it provides conclusions reached through empirical research on the most effective means of reducing instances of individuals pirating software.

Santillanes, G., & Felder, R. M. (2015). Software piracy in research: A moral analysis. *Science and Engineering Ethics*, 21(4), 967–977. <https://doi.org/10.1007/s11948-014-9573-5>

Abstract: Researchers in virtually every discipline rely on sophisticated proprietary software for their work. However, some researchers are unable to afford the licenses and instead procure the software illegally. We discuss the prohibition of software piracy by intellectual property laws, and argue that the moral basis for the copyright law offers the possibility of cases where software piracy may be morally justified. The ethics codes that scientific institutions abide by are informed by a rule-consequentialist logic: by preserving personal rights to authored works, people able to do so will be incentivized to create. By showing that the law has this rule-consequentialist grounding, we suggest that scientists who blindly adopt their institutional ethics codes will commit themselves to accepting that software piracy could be morally justified, in some cases. We hope that this conclusion will spark debate over important tensions between ethics codes, copyright law, and the underlying moral basis for these regulations. We conclude by offering practical solutions (other than piracy) for researchers.

Summary: The authors discuss the inclusion of rule-consequentialist logic (people will be incentivized to create if their personal rights to authored works are maintained) underpinning the basis of intellectual property laws and observe that the blind acceptance of institutional ethics codes may morally justify some cases of software piracy. The authors argue that due to the nature of rule-consequential logic, the moral basis for copyright law, the outcome derived from the rule must promote the best overall consequences. The authors claim that the moral basis for copyrights has created tension between the legal code and the justification given for institutional ethics codes that are

themselves inspired by the legal code; they assert that this issue must be addressed by the scientific and legal communities.

The authors present an example of how this justification might manifest, scientists who work outside of mainstream research institutions who are faced with the choice of becoming criminals by using pirated software due to lack of funding to legally purchase the software or slowing down or stopping their research entirely to comply with the law.

The authors conclude by urging scientists to hold a serious dialogue about the relationship between software piracy and the inefficiencies inherent in intellectual property laws serving to impede the progress of science.

This article is relevant to this study because it offers concrete examples that relay the need to continuously examine our intellectual property laws and ensure the laws evolve as technology advances and changes.

Conclusion

The sources in this study present insights into the threat of software piracy that range in scale from global issues to personal risks. In an effort to assist CIOs, IT managers and IT workers in combatting the threat of software piracy, the source material was aligned into three categories: (a) background and information on digital piracy, (b) piracy prevention methods, and (c) ethics and psychology of piracy. The ultimate goal of the study is to provide information on best practices to reduce acts of software piracy and incorporate these practices into an organization.

Background and Information on Digital Piracy

There are various methods to illegally access software, but regardless of the method, the act of installing or copying software that has not been legally purchased or that exceeds the licensing agreement is referred to as pirating and is an illegal act (Craig & Burnett, 2005). Software piracy is a global problem and in 2015 accounted for 39% of all software installed on computer systems worldwide (Wu, Nan & Li, 2017). In 2007 it was estimated that there was nearly \$35 billion worth of revenue losses due to piracy (Nill & Schultz, 2009). Over a one-year time span from 2010 to 2011, the commercial value of pirated software rose from \$58.8 billion to \$63.4 billion (Han et al., 2014). Gomes et al. (2015) note that software piracy reduces a firm's revenues, as the sale of legal copies decrease in turn. Revenue losses of this magnitude can have secondary consequences of reduced innovation and productivity and result in negative effects on the long-term growth of organizations (Gomes et al., 2015). Governments in many countries have implemented legal frameworks to protect against copyright infringement, yet software piracy is practiced by individuals from all walks of life (Craig & Burnett, 2005).

Software piracy can have consequences beyond legal and financial issues; Craig and Burnett (2005) note that downloading pirated software often results in infection with malware. Many of the sites that provide pirated software copies also harbor computer viruses and spyware (Craig & Burnett, 2005). Kammerstetter, Platzer, and Wondracek (2012) estimate the likelihood of being exposed to malware when using pirated software or games is more than 50 percent.

Software piracy is just one type of digital piracy (Brown, 2014). Brown (2014) advocates that research on digital piracy be broken into categories based upon the type of digital media: music, movies, and software. He notes that people seek out different types of digital media for different reasons; thus, research on digital piracy should also be differentiated based upon media type (Brown, 2014).

Software was not recognized as intellectual property until the Computer Software Copyright Act of 1980, which enabled compiled applications to be copyrighted (Craig & Burnett, 2005). Nine years later the United States Patent Office began to award patents to software developers, which resulted in software developers now having the rights to the compiled programs and underlying source code (Craig & Burnett, 2005). Software developers gained further rights when the No Electronic Theft (NET) Act became law in 1997, amending the definition of “commercial advantage or private financial gain” to include the exchange of copies of copyrighted works, regardless of whether money was paid for the copies (Craig & Burnett, 2005, p. 187). To encourage compliance, severe penalties were assigned to violations of the NET Act: violations are felonies and sentences include up to five years in prison and \$250,000 in fines (Craig & Burnett, 2005). Currently, software piracy is a federal offense and considered to be organized crime (Craig & Burnett, 2005).

Piracy Prevention Methods

Various technical preventative controls have been implemented to reduce software piracy, but researchers have found that many of these controls have had only a minor impact on deterring piracy (Djekic & Loebbecke, 2007). Experiments utilizing a software-based birthmark technology which scans all uploaded and downloaded items through a database of known software programs has shown some promise in identifying, blocking, and removing pirated software, but most of the older versions were found to be too resource-intensive or lacking in strength to be effective; some versions also had to be run manually (Han et al., 2014). Han et al. (2014) note that newer birthmark-based filtering options have not been tested on a large scale for their efficacy.

Beyond the purely technical means of deterrence, research has been conducted in search of strategies that could be implemented to deter pirates (Chiu et al., 2008; Jeong & Khouja, 2013; Wu, Nan, & Li, 2018). Research into customer retention strategies for software developers indicated that strategies that include lower-pricing of software, strong legal consequences for piracy, and reoccurring communication about the negative effects of piracy were effective in influencing consumers' intentions to purchase legal software (Chiu et al., 2008; Jeong & Khouja, 2013). Jeong and Khouja (2013) advocate combining an educational strategy with a strategy that includes lowering software prices or adding value to the software offering. Wu, Nan, and Li (2018) similarly concluded that a *freemium* strategy of offering the base product for free and charging for add-ons increases a firm's market share when compared to the strategy of releasing an updated version of a product that is sold rather than given away. Wu, Nan, and Li (2018) also found that a firm should not try to protect the software with copyright protection when the reservation price for unethical consumers, or those willing to engage in piracy, is relatively low.

Not securing copyright protection for the software in the presence of piracy can reduce price competition, allowing for the higher price for the legally obtained version of the software.

Ethics and Psychology of Software Piracy

Regardless of the legal penalties, employees, students and academics still use pirated software and organizations have been able to do little to stop them because there has not been a clear understanding of why people are motivated to engage in software piracy (Limayem et al., 2004). Part of this misunderstanding stems from the fact that previous research has been overly reliant on economic modeling, which is a limited approach that does not incorporate individual behaviors, or studies based upon data collected utilizing self-reporting methodologies that included a majority of young participants and accounted for the input of very few adults (Brown, 2014). A lack of understanding of the underlying motivations for software piracy did not prevent organizations from creating various techniques to try to deter or prevent the infringement of their intellectual property (Craig & Burnett, 2005).

Two common themes were discovered when research was conducted into the moral and behavioral aspects of why individuals engage in digital piracy (Culiberg et al., 2016). The first finding relates to the moral and ethical aspects (Santillanes & Felder, 2015). The findings from one study suggest that the legal framework meant to deter software piracy is built upon logic that allows consumers to justify piracy in certain instances due to the high cost of software (Santillanes & Felder, 2015). The findings from another study suggest there is a greater utility for one to pirate if the person expects benefits from the use of the pirated materials (Culiberg et al., 2016).

The second theme was concerned with the intentions of the consumer and the variables that influence those intentions (Cho et al., 2015). Results of research showed that there were

negative consequences to overexposing individuals to communications that discourage piracy, as the individuals would interpret the message as an indication that there are a large number of people engaging in piracy and thus justify their intentions to continue in this behavior (Cho et al., 2015). Moral intensity and the perception of negative consequences for piracy were found to positively influence individuals to avoid engaging in digital piracy (Kos Koklic et al., 2016). Individuals who had previously engaged in the act of piracy were found to be more likely to engage in digital piracy (Kos Koklic et al., 2016). The level of education of the individual and ease of access to the software were also found to have positive influential results (Jackman & Lorde, 2014; Kos Koklic et al., 2016).

Final Thoughts

The findings of this Capstone offer insights into the development of strategies that can be implemented at the organizational level to offer protection from the risks associated with software piracy. Organizations should plan to provide all employees with regular ethical and educational training on the risks to the organization of software piracy and the negative consequences for society (Cho et al., 2015; Jackman & Lorde, 2015; Limayem et al., 2004). Organizations also need to create and actively enforce software policies that prohibit the use of pirated software and include the organizational and legal consequences of engaging in this behavior (Cho et al., 2015; Limayem et al., 2004). The goal should be to create an environment where the expectations of the benefits of software piracy are heavily outweighed by tough enforcement of policies that emphasize the negative consequences (Limayem et al., 2004).

References

- Adermon, A., & Liang, C.-Y. (2014). Piracy and music sales: The effects of an anti-piracy law. *Journal of Economic Behavior & Organization*, *105*, 90–106.
<https://doi.org/10.1016/j.jebo.2014.04.026>
- BSA. (2016). Seizing opportunity through license compliance. *BSA Global Software Survey*.
BSA: The Software Alliance.
http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf
- Brown, S. C. (2014). Approaches to digital piracy research: A call for innovation. *Convergence: The International Journal of Research into New Media Technologies*, *20*(2), 129–139.
<https://doi.org/10.1177/1354856513517470>
- Chiu, H.-C., Hsieh, Y.-C., & Wang, M.-C. (2008). How to encourage customers to use legal software. *Journal of Business Ethics*, *80*(3), 583–595. <https://doi.org/10.1007/s10551-007-9456-7>
- Cho, H., Chung, S., & Filippova, A. (2015). Perceptions of social norms surrounding digital piracy: The effect of social projection and communication exposure on injunctive and descriptive social norms. *Computers in Human Behavior*, *48*, 506–515.
<https://doi.org/10.1016/j.chb.2015.02.018>
- Council of Economic Advisors. (2018). *The cost of malicious cyber activity to the U.S. economy*.
<https://permanent.access.gpo.gov/gpo89296/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>
- Craig, P., Burnett, M. (2005). *Software piracy exposed*. Rockland, MA: Syngress Publishing, Inc. <https://ebookcentral-proquest-com.libproxy.uoregon.edu/lib/uoregon/detail.action?docID=254840>

- Culiberg, B., Kos Koklic, M., Vida, I., & Bajde, D. (2016). Examining the effects of utilities and involvement on intentions to engage in digital piracy. *Computers in Human Behavior*, *61*, 146–154. <https://doi.org/10.1016/j.chb.2016.03.029>
- Danaher, B., Dhanasobhon, S., Smith, M. D., & Telang, R. (2010). Converting pirates with cannibalizing purchasers: The impact of digital distribution on physical sales and internet piracy. *Marketing Science*, *29*(6), 1138–1151.
- Djekic, P., & Loebbecke, C. (2007). Preventing application software piracy: An empirical investigation of technical copy protections. *The Journal of Strategic Information Systems*, *16*(2), 173–186. <https://doi.org/10.1016/j.jsis.2007.05.005>
- Gomes, N. D., Cerqueira, P. A., Almeida, L. A. (2015). A survey on software piracy empirical literature: Stylized facts and theory. *Information Economics and Policy*, *32*, 29-37. <http://linkinghub.elsevier.com/retrieve/pii/S0167624515000293>
- Gopal, R. D. & Gupta, A. (2010). Trading higher software piracy for higher profits: The case of phantom piracy. *Management Science*, *56*(11), 1946–1962.
- Han, Y., Choi, J., Cho, S., Yoo, H., Woo, J., Nah, Y., Park, M. (2014). A new detection scheme of software copyright infringement using software birthmark on Windows systems. *Computer Science and Information Systems*, *11*(3), 1055-1069. <https://www.doiserbia.nb.rs/Article.aspx?ID=1820-02141400064H>
- Jackman, M., & Lorde, T. (2014). Why buy when we can pirate? The role of intentions and willingness to pay in predicting piracy behavior. *International Journal of Social Economics*, *41*(9), 801–819. <https://doi.org/10.1108/IJSE-04-2013-0104>

- Jeong, B. K., Khouja, M. (2013). Analysis of the effectiveness of preventive and deterrent piracy control strategies: Agent-based modeling approach. *Computers in Human Behavior*, 29(6), 2744-2755. <http://linkinghub.elsevier.com/retrieve/pii/S0747563213002677>
- Kammerstetter, M., Platzer, C., Wondracek, G. (2012). Vanity, cracks, and malware: Insights into the anti-copy protection ecosystem. In *Proceedings of ACM Conference on Computer and Communications Security* (pp. 809-820).
<https://doi.org/10.1145/2382196.2382282>
- Kos Koklic, M., Kukar-Kinney, M., & Vida, I. (2016). Three-level mechanism of consumer digital piracy: Development and cross-cultural validation. *Journal of Business Ethics*, 134(1), 15–27. <https://doi.org/10.1007/s10551-014-2075-1>
- Mandel, P. & Süßmuth, B. (2012). Determinants of digital piracy: A re-examination of results. *Jahrbücher für Nationalökonomie und Statistik / Journal of Economics and Statistics*, 232(4), 394-413. Retrieved from <http://www.jstor.org/stable/23813539>
- May, C. (2008). Opening other windows: A political economy of ‘openness’ in a global information society. *Review of International Studies*, 34, 64-92. Retrieved from <http://www.jstor.org/stable/20542751>
- McKenzie, J. (2017). Graduated response policies to digital piracy: Do they increase box office revenues of movies? *Information Economics and Policy*, 38, 1–11.
<https://doi.org/10.1016/j.infoecopol.2016.12.004>
- Nill, A., Shultz, C. J. (2009). Global software piracy: Trends and strategic considerations. *Business Horizons*, 52(3), 289-298.
<http://linkinghub.elsevier.com/retrieve/pii/S000768130900024X>

- Panethiere, D. (2005). The persistence of piracy: The consequences for creativity, for culture, and for sustainable development. *The Global Alliance for Cultural Diversity, United Nations Educational, Scientific and Cultural Organisation (UNESCO)*. Retrieved from <http://unesdoc.unesco.org/images/0014/001455/145517e.pdf>
- Ponelis, S. R., & Britz, J. J. (2009). The ethics of piracy in the music industry. *Journal of Information Ethics*, 18(2), 14–26. <https://doi.org/10.3172/JIE.18.2.14>
- Pykalainen, T., Yang, D., Fang, T. (2009). Alleviating piracy through open source strategy: An exploratory study of business software firms in China. *The Journal of Strategic Information Systems*, 18(4), 165-177. <http://linkinghub.elsevier.com/retrieve/pii/S0963868709000420>
- Santillanes, G., & Felder, R. M. (2015). Software piracy in research: A moral analysis. *Science and Engineering Ethics*, 21(4), 967–977. <https://doi.org/10.1007/s11948-014-9573-5>
- Triandis, C. (1980). Values, attitudes and interpersonal behavior. In H. Howe & M. Page (Eds.), *Nebraska symposium on motivation* (pp. 195-259). Lincoln, NE: University of Nebraska Press.
- Wu, D., Nan, G., Li, M. (2018). Optimal software upgrade strategy: Should we sell products or premium services in the presence of piracy? *Electronic Commerce Research and Applications*, 28, 219-229. <http://linkinghub.elsevier.com/retrieve/pii/S156742231830022X>
- Wagner, S. C., & Sanders, L. G. (2001). Considerations in ethical decision-making and software piracy. *The Journal of Business Ethics*, 29(1/2), 161-167.
- Yar, M. (2005). The global ‘epidemic’ of movie ‘piracy’: Crime-wave or social construction? *Media, Culture & Society*, 27(5), 677–696. <https://doi.org/10.1177/0163443705055723>

Yoo, C.-W., Sanders, G. L., Rhee, C., & Choe, Y.-C. (2014). The effect of deterrence policy in software piracy: Cross-cultural analysis between Korea and Vietnam. *Information Development*, 30(4), 342–357. <https://doi.org/10.1177/0266666912465974>