WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Analysis on Cyber Extortion

V. Saraswathi

BBA.LLB(Hons), S. Edhin Frank BA.LLB(Hons)
Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences

ABSTRACT-

This is a comprehensive analysis of the legal frameworks associated with cyber-extortion - the practice of demanding money in exchange for not completing threats to commit harm that might involve a victim's information systems. The author hopes it'll catalyze an urgently needed discussion of relevant public policy concerns. Cyber-extortion has, by all accounts, become a standard , professionalized and profit-driven criminal pursuit targeting businesses. 17% of respondents during a recent survey indicated having received a cyber-extortion demand. a further 13% of respondents weren't sure if their business had received such a requirement . Awareness of the risks of cybercrime has spread. Advancements are made within the field of cyber-security. Furthermore, statutes, regulations and up to date FTC settlements have begun to articulate a minimum standard of care that companies should maintain with reference to the safety of data systems. Yet not all businesses have taken readily available precautions. To complicate matters, cyber-extortions often involve a threat to commit a harm using hijacked networks of computers owned by other businesses. Thus, an analysis specifically dedicated to cyber-extortion is required due to the unique web of liabilities which will arise from a typical cyber-extortion scenario. this text first reviews the available means for prosecuting or recovering damages from a cyber-extortionist. The article then considers the duties and potential liabilities of companies that are victims of cyber-extortion

Keywords: Advancement, criminal, cyber crime, extortion, liabilities

INTRODUCTION

Cyber-extortion—demanding money or something else useful in exchange for not completing threats to commit harm that might involve the victim's information systems—is an evolving and dear sort of criminal activity. The title of this text reflects the very fact that cyber-extortion, just like the proverbial elephant within the room, may be a large problem that has not been thoroughly discussed. this text fills a conspicuous void in existing scholarly and practitioners' literature by comprehensively analyzing the legal frameworks that apply to cyber-extortion and by discussing relevant public policy concerns.The only publicly available survey that has addressed cyber-extortion so far , a 2004 Carnegie Mellon University ("CMU") survey of 100 companies, found that 17% of small and midsize businesses had been the target of some sort of cyber-extortion.an extra 13% of respondents were unsure if their company had been targeted.a standard tactic in cyber-extortion scenarios is to threaten to incapacitate a victim's transactional internet site or other components of its data system this is often referred to as a denial-of-service ("DoS") attack. a method to succeed with a DoS attack—and a way for cyber-extortionists to hide their identity—is to hijack the knowledge systems of unsuspecting businesses or other enterprises and use these hijacked information systems because the tools for incapacitating the targeted victim's internet site or systems.When a network of hijacked computers is employed to overwhelm a victim's system, the attack is named a Distributed Denial of Service ("DDoS") attack. Available evidence suggests that cybercriminals are employing increasingly sophisticated techniques and are increasingly motivated by the pursuit of monetary gain.**aim of the paper is to make people aware about cyber extortion**

OBJECTIVES OF THE STUDY

The present study is to achieve the objectives of the study

- To know about cyber extortion
- To promote proper laws for cyber extortion
- To bring awareness among the public about cyber extortion
- To resolve contradictions about cyber extortion .

REVIEW OF LITERATURE

It bears remarking at the onset that the scarcity of case law on the subject of cyber-extortion so far means legal questions associated with cyber-extortion aren't fully resolved. Specifically, us courts haven't grappled with the liability of execs whose duties include protecting information systems and who fail in those duties when a cyber-extortionist follows through on a threat to disrupt businesses and cause harm. The state of the art in computer security and crime is advancing and awareness of risks has spread.**(Boyce 1997)**Even minimum acceptable standards of care are arguably becoming established.Therefore, to both legal scholars and practitioners, cyber- extortion scenarios present an evolving web of responsibilities and possible liabilities which will demand scrutiny within the coming years. this text will hopefully function as a catalyst thereto much-needed debate.**(Goslin 2019)**The legal and business ramifications of a typical cyber-extortion scenario are often significant, starting from liability for the abuse of personal customer data, to unwittingly allowing one's data system to be hijacked and used as a tool to commit an attack on another company within the context of a DDoS attack. **(Mabunda 2019)**Given the prices related to cyber-extortion and therefore the huge potential pool of malfeasors, targets, and third-party plaintiffs, it's vital to boost awareness of this type of crime, enhance knowledge of legal remedies and responsibilities, and consider the policy implications of holding businesses liable for the safety of their information systems.**(Keshavarzi and Ghaffary 2020)**As defined by the Hobbs Act, extortion is "the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right."As elaborated upon below, extortion is a criminal act under federal and state laws.Cyber- extortion involves the added element of a threat of committing a wrongful act involving computers or information systems.**(Vasiu and Vasiu 2020)** Courts interpret the definition of extortion—specifically, what constitutes a threatened wrongful act—broadly.Blackmail threats, even those that are intended to enforce a legal right may constitute extortion.thus, attempting to embarrass a victim into paying an overdue bill may constitute extortion, as may the attempt to humiliate someone into paying a valid court judgment.**(Лопатина and Lopatina 2014)**Cyber-extortions often consist of three distinct illegal acts: the threat, the act (if committed), and often a preliminary criminal act to make the threatened act credible.**(Rusev 2018)** They controls almost everything from basic communication, finances and even life science . As internet technologies are advancing sooner , more businesses and individuals are storing sensitive data electronically. **(Clutterbuck 1987)**

Internet has become the hunting ground for criminals to form profit, cause disturbance and convey down organizations and governments. Ransomware is that the latest trend that criminals are using for extorting cash from the victims. it's malware that denies you access to your system until you pay ransom**(Ogunyemi and Philosophy Documentation Center 2014)**. Cybercrime has reached to A level that any cyber-attack can cause great levels of extortion. With the support of technology, healthcare organisations are ready to enhance medical treatment assuring better solutions to enhance lifestyle of individuals . Likewise, criminals are interested in the knowledge allocated within hospital and clinics no matter physical or digital storage.**(Thakkar 2017)** Electronic Health Records (EHR) are the foremost important asset in healthcare and criminals are conscious of their value within the black market, including the dark web. This paper analyses the impact of cyber-attacks to healthcare organisations including methods employed by criminals to reinforce their anonymity, and therefore the value of healthcare data nowadays.**(Akhgar, Staniforth, and Bosco 2014)**. It studies blockchain, The Onion Router (TOR) and other common tools to make sure security and privacy while navigating through the web and therefore the reason why cybercriminals cash in of the dark web to sell stolen information from hospitals so as to urge higher gain . It also looks at the amount of extortion that's caused to organisations and the way people are compromised.**(Hernandez-Castro, Cartwright, and Cartwright 2020)** Customary ways to deal with taking character incorporate "dumpster plunging" to recover individual information from disposed of creditcard or service charges, taking individual budgetary letters from post boxes, taking wallets and totes, "shoulder surfing" when people input individual distinguishing proof data, paying off representatives to hand over close to home client data, and physically taking secret records or PC hard drives in which personality data is put away.**(Hadnagy and Fincher 2015)**Online personality cheats assault databases by means of caricaturing (making an impression on a PC from a source that imagines the message is originating from a believed PC's IP address) or phishing(sending an email message to a focused on singular, requesting that the individual get to a Web webpage that imitates a believed organization and afterward uncover private character data). Personality criminals may likewise attempt to break into databases and files in which character data is stored.The spoofer could act like an ISP or even a "fraud counteractive action" specialist co-op.**(Syngress 2002)**On the off chance that the risk of misfortune or robbery can't be stayed away from, anticipation countermeasures can be utilized to diminish the probability that cell phones may be lost or taken and to keep other individuals from getting to and malevolently utilizing the gadgets, information, and remote administrations. Passwords and information encryption are the most generally applied aversion countermeasures.**(Von Ah Morano et al. 2019)**

Numerous sellers can give different countermeasures, for example, client verification, gadget blocking, and remote gadget wipe administrations, to avoid unapproved get to when gadgets are lost or taken. Third, cure countermeasures allude to apparatuses and exercises that endeavor to adapt to the negative outcomes of cell phone misfortune or burglary and to make up for any subsequent harm. For instance, having information sponsored up either on the web or disconnected and reestablished when required are a typical cure. Remote information wipe administrations, get to blocking, remote access to worked in cameras, and GPS following of gadgets can likewise be helpful in such manner.**(Tu et al. 2015)**. Other government rules that effect this region incorporate those forbidding wire misrepresentation and mail fraud9 and those denying interstate transportation of taken property.10 While administrative courts have been hesitant to respect "data" as taken "property" for motivations behind the resolution managing interstate transportation, ongoing cases propose that the issue is still particularly open.**(Warburton 2013)**. Gartner look into directed in April demonstrates that a huge number of customers unwittingly succumb to phishing assaults — email interchanges intended to take purchaser account data, for example, charge card information, places of residence and phone numbers. Purchasers have motivation to be anxious. Phishing assaults undermine their trust in the realness of email originators, compromising customer trust in the very establishment of Internet-based correspondences.**(Hadnagy and Fincher 2015)**

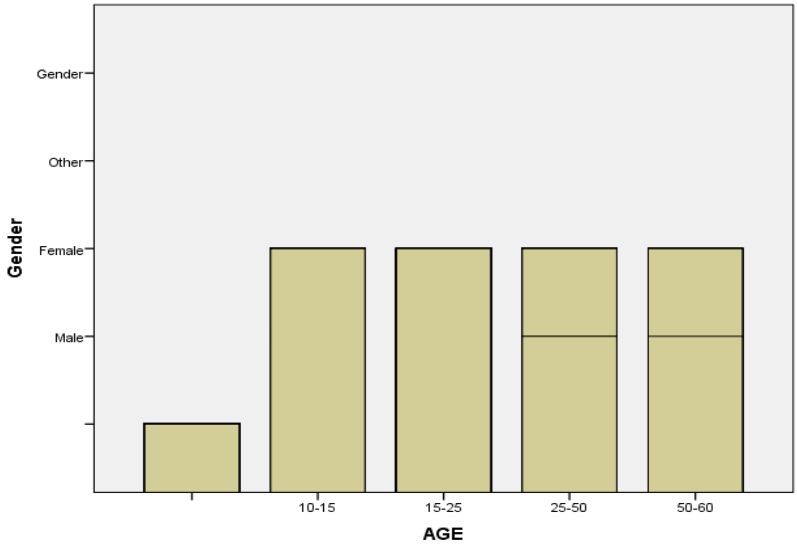
There are various procedures and techniques that character cheats have created to take unfortunate casualties' close to home distinguishing data including low tech (disconnected) and cutting edge (on the web) methods.**(Copes and Vieraitis 2009)**.

Wrongdoers get this data from wallets, satchels, homes, vehicles, workplaces, and organizations or foundations that look after client, worker, patient, or understudy records. Government managed savings numbers give moment access to an individual's close to home data and are generally utilized for distinguishing proof and record numbers by insurance agencies, colleges, satellite TV organizations, military ID, and banks.**(Gill 2006)**.

METHODOLOGY OF THE STUDY

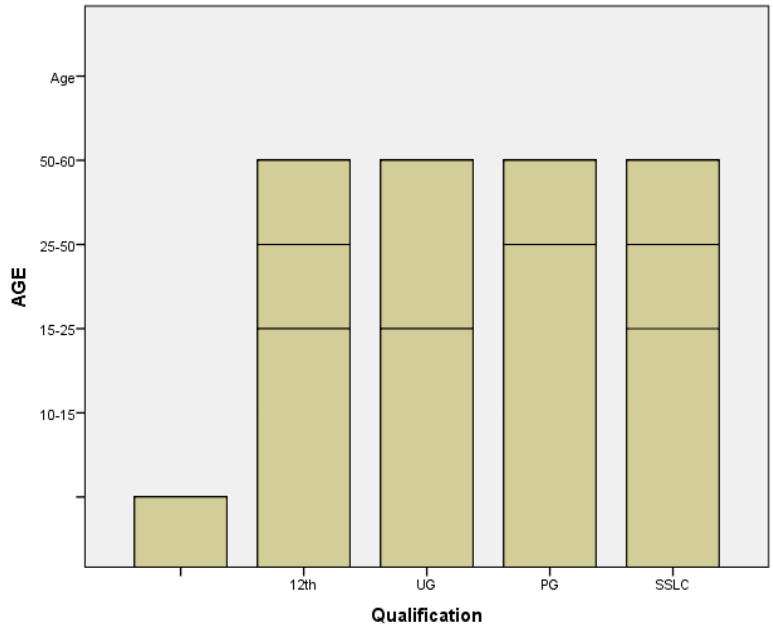
The research method followed here is an empirical research. A total of 200 samples have been taken out of which is taken through a convenient sampling method.The independent variable taken here is age,name,qualification and gender. The dependent variables are to make people aware about cyber extortion .The statistical tools used by the researcher are correlation analysis and graphical representation.Name,age,gender and Qualificatio1.At what level do you agree that people are aware about cyber extortion?2.At what level do you agree harnesses of cyber extortion?

ANALYSIS AND INTERPRETATION



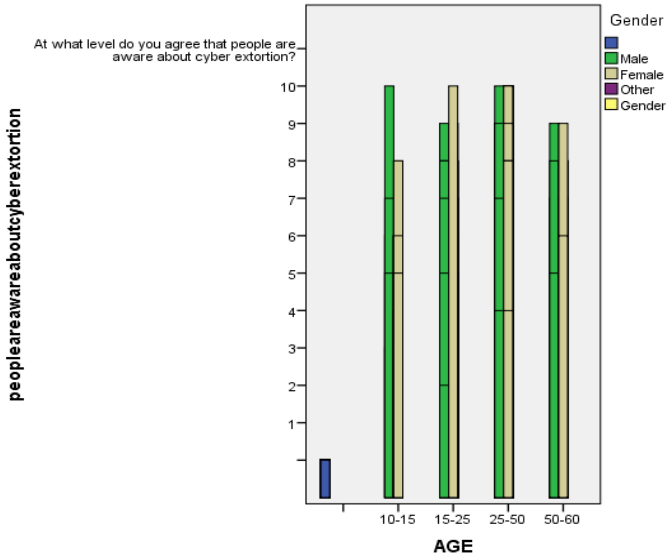
Legend:

The above table represents the age of the respondents who answered the survey,it shows that the people of age group 15 to 25 have given more responses when compared to others.Responses of People below 16 years are 31,age group of 16 to 25 are 47,age group of 25 to 40 are 18 and the responses collected from the people of age group above 40 years are 6.



Legend :

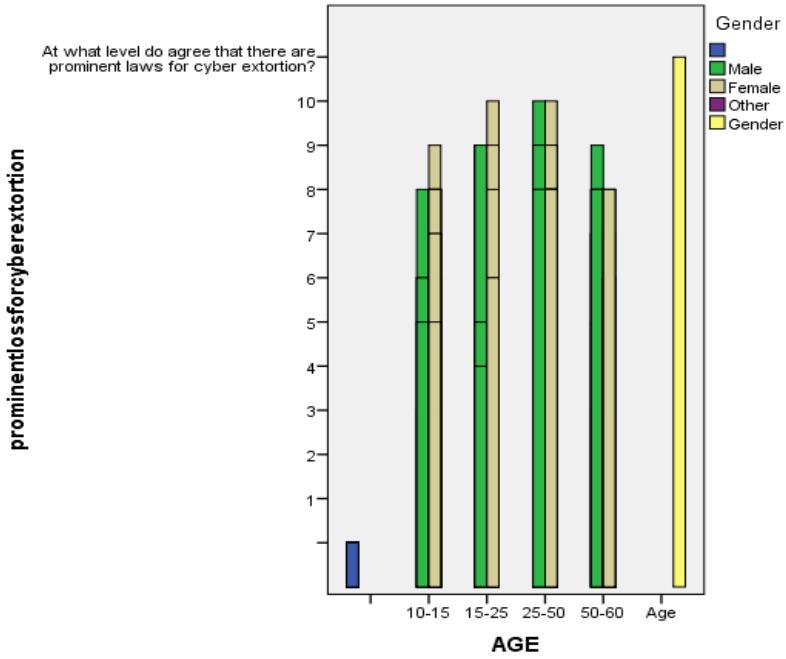
The graph represents the qualification of the respondent to answer the survey it shows that the people who have done PG have given more responses with the bank to other respondents the responses were collected from the people who are qualified with Ug,pg,sslc



Legend :

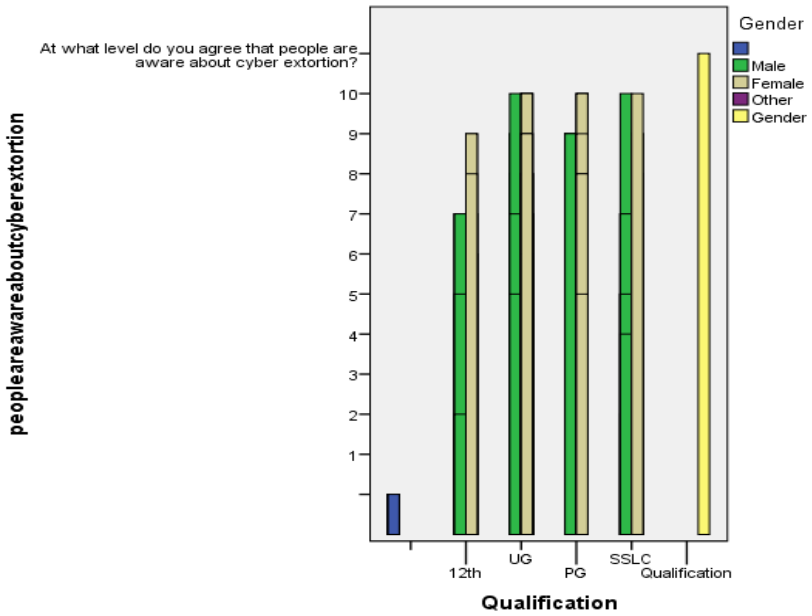
The graph associated with age and gender

As per the responses most people were aware about cyber extortion. As per the graph shows the responses collected from the age group of people 10-15 both female and male have agreed the statement in the level of 7 .the age group of 15 -25 female have agreed the statement in the level of 10 and male have agreed less than 10 and 25-50 age group of people agreed the statement in the level of 10 and 50-60 age group of male have agreed the statement more than the female in the level of 9.



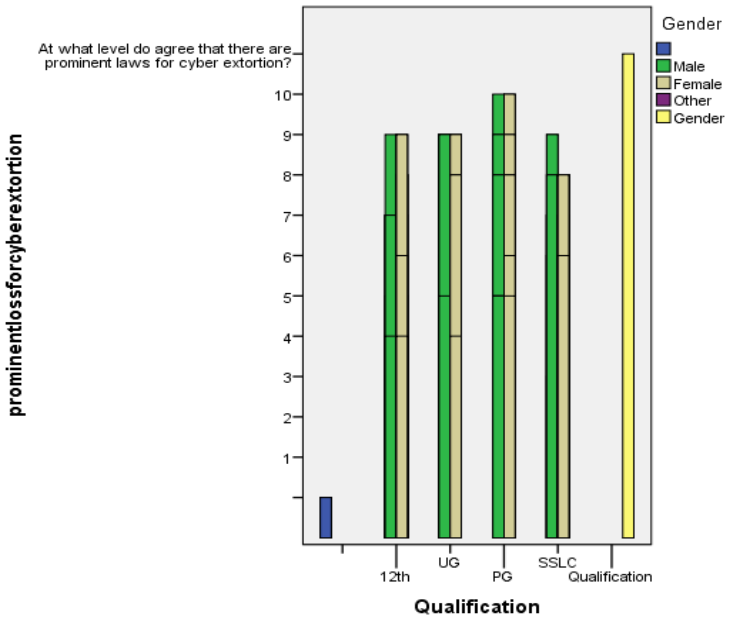
Legend:

The above graph shows the responses of the people in their level of agreeability towards prominent laws for cyber extortion the responses compared with age and gender. As per the responses most people were agree the harnesses of cyber extortion. As per the graph shows the responses collected from the age group of people 10-15 female have agreed the statement in the level of 10.the age group of 15 -25 male have agreed the statement in the level of 10 and female have agreed 9 and 25-50 age group of people female agreed the statement in the level of 10 and male have agreed in the level of 9. 50-60 age group of male have agreed with the statement more than the female in the level of 9.



Legend:

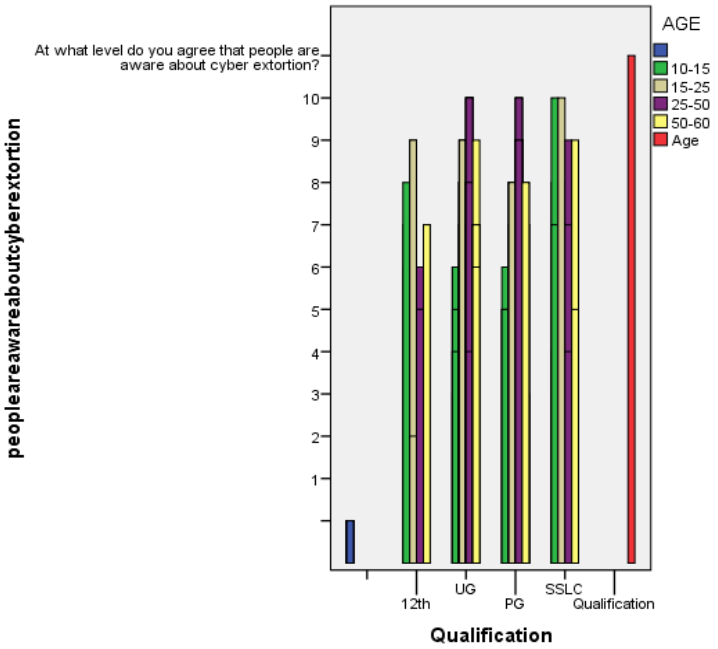
The above graph shows the responses of the people in their level of awareness towards cyber extortion. As per the responses most people were aware about cyber extortion. As per the responses collected from the 12th students female responded more than the male in the scale of 8 and male responded in the level of 7 and the responses collected from the UG and PG students in the level of 10 male have less knowledge about the cyber extortion than the female. female is more aware about cyber extortion as per the responses collected from the qualified PG people moreover SSLC have a less knowledge about the cyber extortion.



Legend:

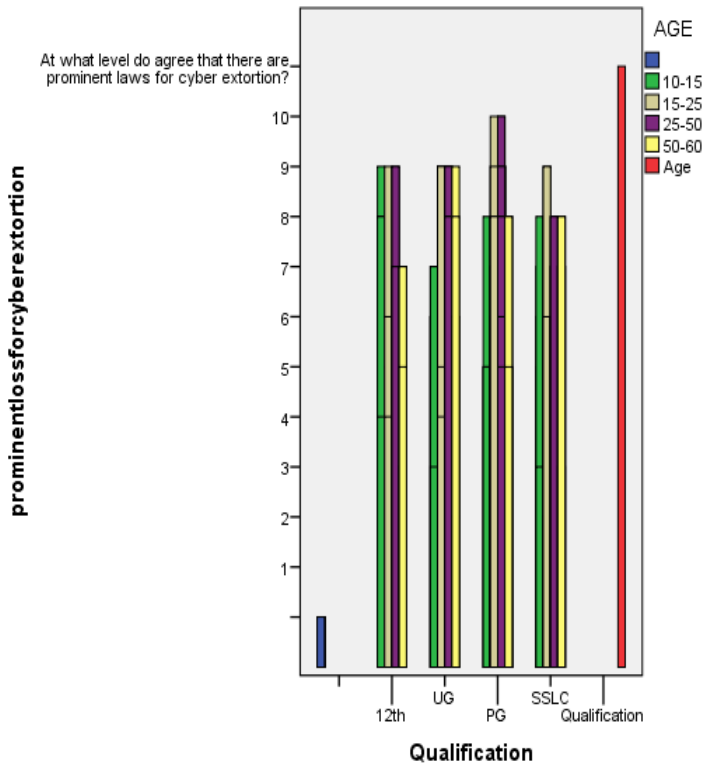
The above graph shows the responses of the people in their level of agreeability towards the statement of the harnesses of r cyber extortion

As per the responses most people were agree the harnesses of r cyber extortion. As per the responses collected from the 12th student are in the level of 10 male have agreed more than the female and UG People have agreed in the level 10 both male and female have agreed in the level of 10 and PG People and SSLC female student have agreed in the level of 10 and male have less agreeability of the statement.



Legend:

The above graph shows the responses of the people in their level of awareness towards cyber extortion. As per the responses most people were aware about cyber extortion. As per the graph that the age group of 10-15 are sslc students in the level of 5 and uG students have known the statement in the level of 7. The 12th and PG People have known the statement in the level of 8 .The age group of 15-25 have agreed the statement in the level of 10 moreover the qualified UG and PG students have agreed the statement more than the others.



Legend:

The above graph shows the responses of the people in their level of agreeability towards the statement there are prominent laws for cyber extortion the responses compared with age and gender. As per the responses most people were agree the harnesses of r cyber extortion. As per the graph that the age group of 10-15 are sslc students in the level of 5 and the UG students have known the statement in the level of 9. The 12th and PG People have known the statement in the level of 8 .The age group of 15-25 have agreed the statement in the level of 10 moreover the qualified UG and PG students have agreed the statement more than the others.the age group of 50-60 have known the constitutional provisions more than the other age group of peoples.

RESULTS

The study states that responses most people were aware about cyber extortion and responses most people agreed were the harnesses of cyber extortion . Hence the objectives of the study are achieved

DISCUSSION

From all the analysis that the Fig 1:As per the responses collected from the 12th students female responded more than the male in the scale of 8and male responded in the level of 7 and the responses collected from the UG and PG students in the level of 10 male have less knowledge about the cyber extortion than the female. female is more aware about cyber extortion as per the responses collected from the qualified PG people moreover SSLC have a less knowledge about the cyber extortion . Fig 2;As per the responses most people were agree that there are prominent laws for cyber extortion .fig 3;As per the responses most people were aware about cyber extortion Fig 4 and 5: As per the graph that the age group of 10-15 are sslc students in the level of 5 and uG students have known the statement in the level of 7. The 12th and PG People have known the statement in the level of 8 .The age group of 15-25 have agreed the statement in the level of 10 moreover the qualified UG and PG students have agreed the statement more than the others.Fig 6:The 12th and PG People have known the statement in the level of 8 .The age group of 15-25 have agreed the statement in the level of 10 moreover the qualified UG and PG students have agreed the statement more than the others.the age group of 50-60 have known the constitutional provisions more than the other age group of peoples.

LIMITATIONS

The major limitation of my studies is the sample frame. The various schemes implemented by each state and education being major drawbacks. Their restrictive area of sample size was also a major drawback.The physical factors are the most impactful and a major factor.The physical factors are the most impactful and a major factor and most of the people are unaware of the laws under IT act.

CONCLUSION

Although the necessity for cybersecurity workers is probably going to still be high, it's difficult to forecast with certainty the amount of workers required or the needed mixture of cybersecurity knowledge and skills.

There are many indications today that demand for cybersecurity workers will still be high, but it's notoriously difficult to live or forecast labor supply and demand for any field, especially one that's as dynamic and fast paced as cybersecurity. Moreover, there are several factors which will affect future need. These include the following:

• How the cybersecurity challenge will evolve as technologies and threats evolve, and the way this might alter workforce capability and capacity requirements.

• How advances—such as better-quality, more-secure software; more productive cybersecurity tools; better training of the workers that operate and manage IT systems; or more robust law enforcement—might change the amount of workers needed in certain roles and alter the talents needed for others.

• what proportion responsibility for cybersecurity might shift from organizations at large to more specialist information technology (IT) or cybersecurity firms, which can reduce the amount or change the combination of cybersecurity workers needed by organizations.

REFERENCES

1. Akhgar, Babak, Andrew Staniforth, and Francesca Bosco. 2014. *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Syngress.
2. Boyce, Brian. 1997. "Cyber Extortion — The Corporate Response." *Computers & Security*. https://doi.org/10.1016/s0167-4048(97)85784-7.
3. Clutterbuck, Richard. 1987. "The Growth of Kidnap and Extortion." *Kidnap, Hijack and Extortion: The Response*. https://doi.org/10.1007/978-1-349-18754-6_2.
4. Goslin, Ian. 2019. "Cyber Extortion Is Threatening Industry 4.0." *Network Security*. https://doi.org/10.1016/s1353-4858(19)30063-7.
5. Hernandez-Castro, J., A. Cartwright, and E. Cartwright. 2020. "An Economic Analysis of Ransomware and Its Welfare Consequences." *Royal Society Open Science* 7 (3): 190023.
6. Keshavarzi, Masoudeh, and Hamid Reza Ghaffary. 2020. "I2CE3: A Dedicated and Separated Attack Chain for Ransomware Offenses as the Most Infamous Cyber Extortion." *Computer Science Review*. https://doi.org/10.1016/j.cosrev.2020.100233.
7. Mabunda, Sagwadi. 2019. "Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill." *Statute Law Review*. https://doi.org/10.1093/slr/hmx028.

8. Ogunyemi, Kemi, and Philosophy Documentation Center. 2014. "How Extortion Works (Evidence From Nigeria)." *Business and Professional Ethics Journal*. https://doi.org/10.5840/bpej2014519.
9. Rusev, Atanas. 2018. "Extortion and Extortion Racketeering." *Oxford Research Encyclopedia of Criminology and Criminal Justice*. https://doi.org/10.1093/acrefore/9780190264079.013.384.
10. Thakkar, Dhanya. 2017. *Preventing Digital Extortion*. Packt Publishing Ltd.
11. Vasiu, Ioana, and Lucian Vasiu. 2020. "Cyber Extortion and Threats: Analysis of the United States Case Law." *Masaryk University Journal of Law and Technology*. https://doi.org/10.5817/mujlt2020-1-1.
12. Лопатина, Татьяна, and Tatyana Lopatina. 2014. "Conditional-Digital Extortion, or Cyber Blacmail." *Journal of Russian Law*. https://doi.org/10.12737/7255.
13. Boyce, Brian. 1997. "Cyber Extortion — The Corporate Response." Computers & Security. https://doi.org/10.1016/s0167-4048(97)85784-7.
14. Clutterbuck, Richard. 1987. "The Growth of Kidnap and Extortion." Kidnap, Hijack and Extortion: The Response. https://doi.org/10.1007/978-1-349-18754-6_2.
15. Goslin, Ian. 2019. "Cyber Extortion Is Threatening Industry 4.0." Network Security. https://doi.org/10.1016/s1353-4858(19)30063-7.
16. Keshavarzi, Masoudeh, and Hamid Reza Ghaffary. 2020. "I2CE3: A Dedicated and Separated Attack Chain for Ransomware Offenses as the Most Infamous Cyber Extortion." Computer Science Review. https://doi.org/10.1016/j.cosrev.2020.100233.
17. Mabunda, Sagwadi. 2019. "Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill." Statute Law Review. https://doi.org/10.1093/slr/hmx028.
18. Ogunyemi, Kemi, and Philosophy Documentation Center. 2014. "How Extortion Works (Evidence From Nigeria)." Business and Professional Ethics Journal. https://doi.org/10.5840/bpej2014519.
19. Rusev, Atanas. 2018. "Extortion and Extortion Racketeering." Oxford Research Encyclopedia of Criminology and Criminal Justice. https://doi.org/10.1093/acrefore/9780190264079.013.384.
20. Thakkar, Dhanya. 2017. Preventing Digital Extortion. Packt Publishing Ltd.
21. Vasiu, Ioana, and Lucian Vasiu. 2020. "Cyber Extortion and Threats: Analysis of the United States Case Law." Masaryk University Journal of Law and Technology. https://doi.org/10.5817/mujlt2020-1-1.
22. Лопатина, Татьяна, and Tatyana Lopatina. 2014. "Conditional-Digital Extortion, or Cyber Blacmail." Journal of Russian Law. https://doi.org/10.12737/7255