Public Safety's Perception of Cybercrime: A Pilot Survey of Victimization and Experience Across Age Groups

Robert G. Cotton

A.S. in Computer Science, Georgia Perimeter College, 2009
B.S in Information Technology, Middle Georgia State University, 2018
M.S. in Information Technology, Bowling Green State University, 2020

A Research Paper Submitted to the School of Education and Behavioral Sciences

Middle Georgia State University

In partial fulfillment of the requirements for the degree of

DOCTOR OF SCIENCE IN PUBLIC SAFETY

Macon, Georgia

December 2025

Public Safety's Perception of Cybercrime

Robert Cotton

SFTY8980: Evaluation Planning and Design

Dr. Mathew M. Caverly

November 14th, 2025

Chapter 1: Introduction

The world has become reliant on the use of information technology systems for individuals' daily activities. Whether it is at work, for entertainment, or just daily commerce, technology's omnipresent nature has never been more apparent. As these systems continue to increase in size, their vulnerability to attack and the impact on communities when they are compromised increases as well. With over $445 billion lost annually from cyber-attacks on larger organizations, and untold amounts that have been lost by smaller attacks which go unreported, it is necessary to gain a better insight of municipal public safety official's perception and understanding of cybercrime and other crimes that leverage technology (Samanti, et. al., 2017)

Employees within the public safety sector are no exception to this explosion of technology. From the day-to-day use of high-end technologies, such as Computer Aided Dispatch, body worn cameras, license plate readers, and online cloud platforms that allow for the search of pawn shop databases, public safety officers must be proficient in the use of a multitude of technology systems. But it doesn't stop there. Public safety officers must also possess knowledge and understanding of cybercrime, and other crimes involving technology, in order to properly confront these crimes at the local level.

Public perception of large cyber-attacks and cybercrimes were once thought of as being mostly fictional movie plots, targeting governments or large corporations. Large attacks that make headline news like the Equifax breach in which 148 million records were stolen from over 200,000 individuals often overshadow daily cyber-attacks. As technology becomes a more effective vehicle for exploitation and crime it is necessary to remind ourselves that there are many more victims that do not make headline news (Swinhoe, 2020). Large scale attacks once made up the majority of cyber-attacks. This is no longer the case with the rise of technologies, such as blockchain, that allow anonymous funds transfer. With the recent rise in popularity of ransomware attacks, cybercrime can easily target small businesses, older members of communities, and anyone else that is careless enough to open an email attachment by mistake. In the modern era, no target is too large or too small.

As more aspects of our daily lives are experienced through the digital world, the omnipresent threat of cyber-attack looms over all of us. Any digital service an individual logs into, at any time, is subject to those threats, whether it be our phones, bank accounts, online storefronts, or countless social media accounts. Any one of these services could be the target of a crime that would require police intervention of some kind (Marta, 2024) (Kamuda, 2018).

In 2008, the creation of a cryptocurrency titled Bitcoin allowed for the anonymous transfer of money (Richardson, 2017). Richardson argued that this novel technology enabled new areas of cybercrime and the explosion of occurrences. Prior to 2008, profiteering from cybercrime required the exploitation of gift cards which were risky, easily traceable by law enforcement, and subject to cancellation or termination if caught in time. Research in 2016 discovered that financial impacts from cybercrime from 1997-2006 averaged $12.18 billion per year in losses (Guo, 2016). In the 12 months following July 2011 it was discovered those losses increased by a factor of 10.

New electronic currency, like bitcoin, has led to an explosion of cybercrime, and the facilitation of more conventional crimes. Illegal activities are no longer just conducted using cash, a host of other technologies are used to cover their tracks. Including PayPal, Venmo, CashApp, AliPay, and Wise, not just cryptocurrencies such as bitcoin (Gomez, van Liebergen, & Caballero, 2023).

Ransomware alone has become such a large portion of overall cybercrime. Crime syndicates have created a business model around providing such services to other less technologically advanced crime syndicates. This new business model dubbed "Ransomware-As-A-Service" (RaaS), is now the preferred method for crime syndicates to attack their victims (Hull, 2019). Hull estimates that an average of 3% of individuals pay the ransom when their computers are attacked, yielding criminals millions of dollars for every successful ransomware campaign that is launched. Another famous virus "WannaCry" infected 300,000 computers worldwide and extorted $300-$600 ransoms for each infection (Stewart, 2018). Often referred to as the gold standard of malware, the "CryptoLocker" ransomware campaign that was launched in 2013, utilizes well-made phishing emails designed to mimic common FedEx and UPS emails to target users and extort ransoms from unsuspecting individuals (Richardson, 2017).

Ransomware no longer exclusively targets large corporations. As corporate cyber defenses improve, criminals have started targeting the public at large looking for smaller, but easier "pay days" (Richardson, & North, 2017). Public safety officers need to be trained and equipped to assist and know their limitations when assisting the public in these situations.

The global nature of cybercrime is causing ordinary citizens to become more engaged, aware, and involved in discussions about prevention (Arstanbekov, et. al., 2024). As interest swells from citizens and community members, government officials and public safety personnel must struggle with the criminal justice aspects of prosecution and prevention. But major questions still loom; Do local public safety personnel have the experience and expertise to adequately combat cybercrime? Do they fully grasp the community's concerns versus more traditional crimes?

With the ever-evolving attack vectors in cybercrime and the advances in technology, local law enforcement must now have an understanding of technology enough to respond and protect their community against cybercrime. Public safety professionals must now be more versatile than ever, utilizing new technologies that are becoming standard within their industries and combating crimes which use other types of evolving technologies. Not only must a police officer be proficient in the usage and functionality provided by their body camera, but they must also have a working knowledge of advanced software tools to uncover and retrieve evidence from smartphones.

As the complexity of technology grows, so must the understanding of our public safety officers, not just to leverage the technology, but to fight instances of crime that may arise as a result of that technology or through the use of that technology (Snell, 2019). Public safety members cannot be bystanders to the constant advancement of technology. They must be diligent to take an active role in learning and understanding new technologies so that when instances of crime arise from their use, they are prepared to combat it.

The ever-changing nature of technology, both from a criminal aspect and crime prevention aspect, lends itself to be more digestible by younger generations that grew up with and are thereby more familiar with the various base components of the technology (Mollborn, et. al. 2021). The data suggests that this assumption is incorrect, and that age groups are equally impacted by cybercrime.

An individual's understanding of technology and cyber security influences their perception of cybercrime, when that individual is a member of a local public safety organization it can also affect the outcomes for the community. To what degree does age affect public safety personnel perceive the severity of and the occurrences of cybercrime within their organization and the community? Is their understanding of technology only as deep as their day-to-day use of the technologies that are required to perform their duties or is it a more thorough perspective that helps to benefit the community?

Inadequate awareness of local law enforcement, lack of communication from management, underuse of federal resources, and lack of communication with the public are all areas of necessary improvement. Inadequate awareness from law enforcement can be explained through lack of training, or knowledge of new technologies, contributing to slow responses to cyber dependent crime and sometimes even non-response.

To quantify public safety employees' perception of cybercrimes, the distributed survey was contrasted against existing survey data from the Crime Surveyfor England and Wales to provide insight into how officers have been impacted by cybercrime. The survey also encompasses public safety professionals' opinion of cybercrime both on the job, and in their personal lives. With this information, the comparison of variance between the groups is made, looking for statistical anomalies in the f-values between the age groups of the public safety officers.

In understanding new technologies to fight crime, so to must public safety officers understand the technologies that are used to commit crime. To what extent do public safety officers understand the nature of cybercrime? Have they been victims, and does that victimization influence their perceptions of cybercrime? Does age play a factor in these differences?

One may assume that younger officers are less frequently personally impacted by cybercrime because they are more familiar with the ever-changing technological landscape (Mollborn, et. al. 2021). To test this question, the survey tests across six age groups within a public safety organization, asking whether or not an individual has been impacted by some element of cybercrime. Additionally, attempts to quantify the element of cybercrime to determine how many times that age group was impacted, and to what extent.

Relevant Background

While globalization and the cybercrime that originates from foreign states is a factor, it is important to note that many researchers and policy makers recognize this as a problem. There have been concerted efforts to reduce cybercrime or crimes that require technology through well formulated policy. The effectiveness of these policies is unclear, but training initiatives and collaboration between public safety and community members is underway on a global scale. As such, agencies at the federal level get most of the attention and sparse resources necessary to combat cybercrime. As more cybercrime takes place and impacts local communities, this paradigm has shifted from a focus of cybercrime at an international and large corporation level, to a more localized level.

As a result, there has been a push to create task forces at the local level specifically to aid citizens and entities within their jurisdictions to fight local cybercrime which is on the rise (Taylor, 2023). These task forces focus on combatting child pornography, exploitation, bullying, and stalking. Other types of cybercrime that are higher profile such as those that may obscure drug trafficking, wire fraud or threats to national security are pushed back to federal agencies to investigate.

Even though cybercrime is on the rise, there is a lack of support from upper management in many local agencies to provide resources to combat them. This coupled with a lack of training to patrol personnel and “boots on the ground”, insufficient technical expertise, and lack of access to the tools and equipment to properly investigate cybercrimes create additional challenges at the local level. Officers who are capable and have been trained in fighting cybercrime face the additional challenges of being unable to access informational resources to use the technical expertise and equipment that exist at the federal level. There is no single source of information that contains all the federal resources that are available to an officer. Instead, the federal experts and the advanced labs, technology, and forensic equipment are underutilized by local law enforcement simply because of a lack of communication structure to know of their existence.

Federal programs, such as the Secret Service’s National Computer Forensics Institute (NCFI), exist to aid in the training of State, Local, and Tribal law enforcement members (Cyber Investigations, 2025). These programs are in place to help not just law enforcement, but judges, prosecutors and the justice system as a whole to better understand and combat the ways in which cyber criminals exploit computers, mobile devices and the internet. The NCFI focuses on emerging technologies and related crimes by providing various levels of training to law enforcement personnel.

Plan for Organization

This paper is organized into nine distinct categories, an executive summary and introduction, including this plan are used to orient the reader and to provide context. The ever-evolving nature of technology, and the crimes that are committed that are reliant on those technologies create an amorphous subject that evolves as technology progresses. (Stewart, 2018). Summarizing key information to the reader is imperative to ensure that readers are oriented to the technological space at the time of the paper's construction. Following the orientation of the reader, they will be presented with the thesis, is age a factor in a public safety officer's understanding of cybercrime? The independent variable, the age group, will be evaluated against officer's responses of if they have been victims of some element of cybercrime.

Following the introduction, the problem itself will be further discussed by examining other research into victimization of not just public safety personnel, but members of the public. Further theoretical discussion will investigate the perceived severity of cybercrimes, along with if cyber-related, cyber-dependent, and cyber-adjacent crime severity effects perception. This will be accomplished reviewing similar work by in the United Kingdom in which nationwide studies asked respondents if they had been affected by cybercrimes, then compared those results to conventional crimes. (Arstanbekov, et. al., 2024) (Button, et. al., 2025) (Hadlington, et. al., 2021). Cyber-related questions from this national study are asked to the respondents so that the results can be examined within their respective age groups. The details of this study, and how it has been adapted into this study are examined in the design methodology along with material differences that may result anomalies in conclusions.

Lastly, attempts to compare those results in the potential findings are examined to determine if, to what degree, age factors into a public safety officer's perception of cybercrime. Real world applications and implications of these results are examined and how much of a factor they could play into the daily jobs of the officer. Potential solutions, such as training, will also be examined to attempt to mitigate any negative findings, or inversely, indicate that active training is effective in preventing age-based victimization.

Chapter 2: Literature Review

A recurring theme of the difficulties of combating cybercrime due to the nature of its globalization is apparent in much of the research (Arstanbekov, et. al., 2024) (Button, et. al., 2025). Arsanbekov and Button's research helps to highlight the need for research into the perception of the victim on the crimes that are impacting them. While both studies indicate that this perception is changing, it is unclear how long these changes in perception will take.

Cybercrime does not know or respect international borders, as such, state and local roles in combating cybercrime have always been somewhat questionable (Taylor, et. al., 2023). Taylor goes on to discuss what roles local and state police should play in technologically based crime and cybercrime. It is noted that much crime now has an element of cyber or technology. Bullying, stalking, and other threating behavior now often occur virtually through social media or a communications platform. While lack of law enforcement awareness in these platforms plays a factor in how these events are prosecuted, it is uncertain if outcomes are similar across different communities. What is clear is that community-oriented policing efforts such as community outreach are necessary to ensure that those perceptions are changed.

Research on attitudes towards cyber security and relative knowledge of the individual about the subject have shown that risk increases to cyber events increases with the lack of knowledge about technology (Hadlington, 2018). As noted, lack of knowledge creates "passive engagement" which tends to exacerbate victimization in more traditional crimes that have an element of cyber or technology that is not fully understood by law enforcement.

The 2021 crime survey for England and Wales sought to better understand this same issue within the age groups of their citizens. The information collected was combined with additional victim research and first-hand accounts to get to the root of why the perception of cybercrime and technological crimes are somehow viewed as less severe than their physical counterparts

(Button, et. al., 2025). While interviews with victims indicated that public safety officials do not do an adequate job of reporting and combating instances of cybercrime, the public perception from survey data indicates that the perception of severity is on the rise (Hadlington, et. al., 2021).

In other research by Hadlington in 2021, he and his team explore police experiences and perceptions of cybercrime in the United Kingdom. It is noted that in the underlying research that crimes that are cyber dependent were perceived to be less severe than similar crimes that were cyber enabled (Hadlington, et. al., 2021). Additionally, lack of distinction and clear boundary definition between cyber crimes that are 'cyber-enabled' and 'cyber-dependent' creates ambiguity when discussing the topic both with academics and crime fighters. This ambiguity created difficulties in interpreting results, with participants often being confused by the discussions.

The "passive engagement" issue is compounded by a lack of understanding of the nature of certain crimes and their cybercrime counterpart. The issue at hand is that crimes can be cyber-enabled or cyber-dependent. For example, fraud can be committed with or without a technological component, however computer fraud is cyber enabled. Cyber dependents are only made possible through the use of technology, for example, computers. The proposed survey taken from questions on the Crime Survey for England and Wales (CSEW) survey will attempt to make a distinction between cyber-enabled and cyber-dependent crimes in those results to see if there is a perception difference in the perceived severity of those crimes (Button, 2025) (Furnell, 2002).

Much of what we hear and see regarding cyber crime seems to originate on the news from high profile attacks such as the Colonial Pipeline hack in 2021, STUXNET in 2005, the Equifax Breach, and the Ukrainian power grid attack in 2015 (CISA, 2025). The vast amount of literature surrounding cybercrime almost exclusively focuses on the international and business perspectives of cybercrimes (Stewart, 2018).

The Equifax breach of 2017 compromised the personally identifiable information of millions. After the breach, the subsequent lawsuit determined that negligence on behalf of Equifax enabled the cyber criminals to easily gain access to the data by leaving default passwords on critical data and systems (Glenn, n. d.). However, data theft is not the only crime that cybercriminals commit. In the Colonial Pipeline attack in 2021, hackers used ransomware to lockout key systems that controlled the flow of gas in the southeastern United States. The attackers would not release access to the system until a ransom of $4.4 million in the cryptocurrency, Bitcoin, was paid. (Biden Signs Cybersecurity Executive Order Following Colonial Pipeline Hack., 2021)

Not all cybercrime attacks are launched by organized crime, some are perpetrated by nation states, or nation-states proxying as an organized crime syndicate. The Stuxnet worm, which is widely believed to be a joint United States and Israeli venture targeted centrifuges in the Iranian nuclear refinement program. The worm, which caused centrifuges to catastrophically fail, was sophisticated enough to report incorrect readings to operators that mimicked what correct readings would look like to an operator making the cause of the failures impossible to detect. This attack set the Iranian nuclear program back an estimated 10 years (Vanlyssel, 2025). In 2015, Russia, as a precursor to invasion and the annexation of Crimea, launched numerous assaults on the Ukrainian power grid. These attacks, along with a misinformation campaign sought to destabilize Ukraine, and sow discontent in the citizens towards the leadership. The attacks resulted in thousands left without power for days, and a perception of the public that government leadership was corrupt or incompetent (Vanlyssel, 2025) (Russia renews big attacks on Ukrainian power grid using better intelligence and new tactics., 2024).

These high-profile attacks offer a false sense of security that cybercrime only targets governments or large organizations. This is patently false, and cybercrime targets all demographics with no regard for size or industry (Stewart, 2018). Stewart goes on to discuss that smaller cybercrimes often go unreported or misreported because of lack of jurisdictional understanding in law enforcement, or a sense of helplessness in the victim. Proper training in public safety when responding to smaller crimes at the local level can assist in correctly reporting this information.

This plethora of literature about cybercrime exists for businesses and governments, but little is focused on the local crime fighting response, with notable exceptions. Foreign countries, perhaps due to law enforcement structure, or local perceptions of cybercrime, have emergent areas of research on the topic. India, Pakistan, Ukraine, Serbia and Turkey all have such literature that delve into practical training aspects and awareness regimens (Arstanbekov, et.al., 2024) (Kamuda, 2018) (Richardson & North, 2017) (Marta, 2024) (Taylor, et. al., 2023) (Milojević, S., Milojković, B., & Janković, B., 2025). Literature reinforces the idea that there are wildly differing views on cybercrime at the global level that contribute to the challenges of combating it and educating on the subject.

In the United States, lack of training for public safety at the local level, and not enough resources at the federal level is a key takeaway from the research (Whittaker, 2018) (Swinhoe, 2020) (Snell, 2019) (Ellis, 2016). Foreign research into the subject of technological training is quite the opposite and suggest that theoretical and practical application of new training methodologies is necessary to keep up with the rapidly advancing technology changes

(Milojević, S., Milojković, B., & Janković, B., 2025). (Kussainova, Z., Sartbekova, N., & Abakirov, A., 2025).

A recurring theme in the literature is that there are differences in training and awareness at a global level between countries, and even continents. But those differences are minor when compared to training and awareness at a domestic level; and digital literacy through hands on vocational training is rare domestically, unless it is provided through specific vendors that are experts on the applicable technology (Kussainova, Z., Sartbekova, N., & Abakirov, A., 2025).

Chapter 3: Methodology

Button's research into the seriousness of cybercrime in the United Kingdom took a victim first approach by examining the perceptions and firsthand accounts into various types of conventional crime and evaluating if there was a cyber or technological component (Button, et. al., 2025). Their research sought to answer the question: does law enforcement view various types of cybercrime as less serious than conventional crime of the same severity? After all, fraud is fraud regardless of whether the fraud was committed through a computer. Their research ponders that question, and goes on to ask: if this is the case, then why? Does the vector of the crime impact its perceived severity to law enforcement officers? In other words, by performing similar research, but placing the "shoe on the other foot" by asking public safety the same questions that is asked to victims we are better able to understand public safety personnel's perception of cybercrime.

This proposal relies heavily on work from Button et.al. 's work in *The case of computer misuse crime in the United Kingdom and the victims' perspective* and the survey design that has been conducted by the Office for National Statistics in Britain. These works provide the framework for this proposal. The survey that was generated for this proposal remains as close to the 2017-2018 Crime Survey as possible for it to be relevant to American members of public safety. By doing this, additional opportunities to analyze this survey's data against the work done in the United Kingdom.

The research accomplishes this by analyzing data from the 2018 Crime Survey for England and Wales Questionnaire, and focusing on specific cyber, computer, and virus-related crime of the respondents (Office for National Statistics, 2018). The questionnaire is a victimization survey of individuals, which showed a large increase in computer related offenses and the perceptions of those victims on the severity of the crime.

This research proposal adopted a similar methodology of asking public safety officers, who are also victims of cybercrime, about the nature of the attack and the seriousness of those crimes that they have experienced. Those same questions were asked to members of public safety: law enforcement, fire, and EMS from a personal perspective. The results were used to compare victimization, by age groups of the respondents using a one-way ANOVA test against non-public safety personnel. The survey questionnaire asked the same questions from the original Crime Survey for England and Wales Questionnaire as it relates to basic demographics, technology, cybercrime, computers, hackers, viruses, and online fraud.

A comparison was made using a one-way Analysis of Variance ANOVA between survey takers. Those survey takers were broken into the following age groups: Under 25, 25-34, 35-44, 45-54, 55-64, and over 65. Then they were evaluated to determine if there is a difference of significance in the rate of cybercrime victimization in the age groups of the new survey using f-value comparisons.

The groups were compared using selected questions on cybercrime, cyber fraud, hacking, and viruses from the Crime Survey for England and Wales (CSEW). All questions were as similar to the original CSEW survey as reasonably possible, with any differences, and the reason for those differences documented, so that later research can be performed by comparing the original results of the CSEW to any new results contained in this survey. The questions in the new survey retained the original question encoding, e.g. **FV81**, to aid in any future research comparisons that are made.

The questionnaire was voluntary and unpaid. It was distributed through upper management within various public safety organizations in the State of Georgia. However, responses outside of the State will not be counted to gain a better understanding of cyber-enabled crime, and cyber-dependent crime and how it affects members of public safety within the state. Additionally, the severity of those instances was examined, how they occurred, and similarities and trends between types of attacks that public safety may experience. This was done to gain a better understanding of what types of attacks non-public safety members may be vulnerable to.

A full breakout of all questions and the corresponding chapters is listed below. Each chapter is discussed individually for their significance in the parent research and the research being proposed. Additionally, and most importantly, any changes to the individual questions necessary for comprehending the questions will be discussed, along with potential impacts to the results.

Questionnaire: Demographics Chapter

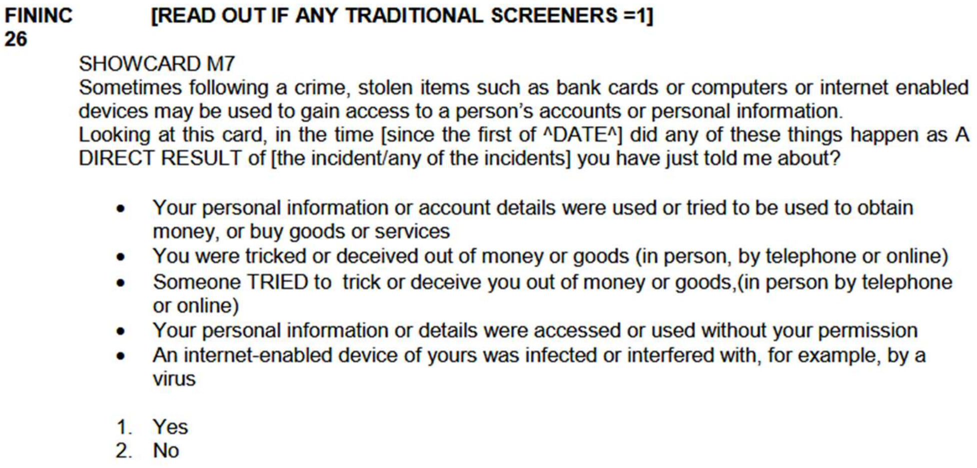
The questions from this chapter will seek to identify commonalities in the groups. Changes will be grammatical localization changes to be more understandable by American respondents. As an example, question to determine the respondents age will be changed from "could you please tell me which age band you/(name) is in?" to "could you please tell me what age you are?". Any other demographic questions on sex, name, date, and marital status will be unchanged. Additionally, the number of possible responses will be reduced from ten age groups to six to reduce confusion for respondents.

Questionnaire: Fraud Chapter

This chapter will begin with the same introduction from the questionnaire of: "The next set of questions relate to fraud; including being tricked out of money or goods, misuse of your personal details, unauthorized access to your bank, email or social media accounts, computer viruses and so on". This will be done to establish context for what is to follow for the respondent, in addition to mimicking actual survey takers from Britain and Wales.

All questions within this survey are asked by the surveyor, and the respondent is asked to respond to them. These will be rephrased to simply ask the respondent rather than to respond to a person administering the survey. These changes are cosmetic and should have a minimal impact on the results.

A question to determine how the individual has been financially impacted by cyber fraud will be asked. This question seeks to establish instances of fraud and the source of that fraud and whether it was cyber dependent, or cyber related. Since it is a multifaceted question, careful interpretation will be needed when analyzing questions that tie results together to determine the nature of the financial loss, i.e. through fraud, viruses, or stolen personal information. Since this proposed survey is much more focused on cyber aspects of crime, the broadness of this question may be overlooked. A series of financial cybercrime questions will be asked as a follow-up to the initial cyber question that determines if there is an occurrence of financial loss with a cybercrime to establish frequency of any occurrences. No additional changes in wording will be made to this question. Questions determining the loss of personally identifiable information will be asked to establish to what degree the individual was impacted by elements of fraud identified in any questions that determine financial loss. No additional changes will be made to these questions.



FININC 26 **[READ OUT IF ANY TRADITIONAL SCREENERS =1]**

SHOWCARD M7
Sometimes following a crime, stolen items such as bank cards or computers or internet enabled devices may be used to gain access to a person's accounts or personal information.
Looking at this card, in the time [since the first of ^DATE^] did any of these things happen as A DIRECT RESULT of [the incident/any of the incidents] you have just told me about?

- Your personal information or account details were used or tried to be used to obtain money, or buy goods or services
- You were tricked or deceived out of money or goods (in person, by telephone or online)
- Someone TRIED to trick or deceive you out of money or goods,(in person by telephone or online)
- Your personal information or details were accessed or used without your permission
- An internet-enabled device of yours was infected or interfered with, for example, by a virus

1. Yes
2. No

Depending on the responses given, the survey will be programmed to ask follow up questions to the questions in the financial series to determine the nature of fraud. The follow-up questions asked will be relevant to cyber-enabled and cyber dependent crimes. A question determining whether money or property was lost. A follow-up question to establish if additional secondary losses resulted followed by questions to determine if threats were made. Lastly, a question will be asked to establish if the event was sexual in nature. No changes in the wording of these questions will be made.

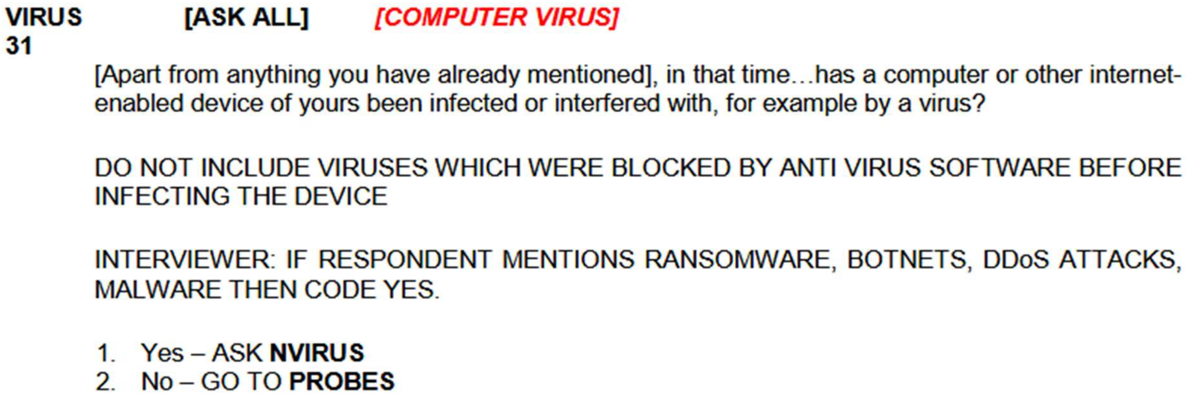
The fraud series of questions seeks to determine how the perpetrators benefited from the incident, the first question will be asked to determine if any purchases were made. Followed by two linked questions that will be asked. If a positive result to from the first is received it will be used to determine if the benefit was from the victim's bank or credit card. The subsequent question will determine if the nature of the fraud was identity theft. Finally, a question will be asked to determine if a more traditional type of fraud occurred, such as a fake investment.

Three questions will be asked in succession to establish if the fraud was through social engineering. Lastly, two questions will be asked to determine the technical aspects of the offense and if secondary events contributed to the original attack or if additional victimization took place.

The next series of questions will be asked to establish instances of social engineering through technological means. With follow up questions being asked to determine the severity and frequency by asking the number of occurrences. These questions will be modified to ask greater than or less for the number of occurrences. This is because of limitations in the survey software being utilized. It is unknown what effect this will have on results but will have a lesser impact for the number of positive answers to the social engineering questions because they are a prerequisite.

A question will be asked to establish instances of virus infection or account compromise that led to loss of the individual's PII (Personally Identifiable Information). All results from this question and all related follow-up questions will need to be scrutinized as to their applicability to American respondents. The original questionnaire was aimed at citizens of Wales and Britain that fall under the General Data Protection Regulation (GDPR) of the European Union (EU). As such, respondents have a different understanding, expectation, and legal framework for the handling of data that would result in the loss of privacy (Gioia, Lener, 2024). Per Article 4 of EU 2016/679 of the GDPR "any information relating to an identified or identifiable natural person." is subject to various protections and requirements that American respondents would not enjoy. This will likely result in American respondents viewing follow-up questions attempting to establish severity as less severe than their European Union (EU) counterparts.

The next question will seek to establish from the respondent the attack vector and nature of the aforementioned loss of Personally Identifiable Information (PII) and virus infection line of questioning. Follow-up questions to the viral infection question will establish frequency and severity of virus attacks on the individual. By asking the number of viruses attacks the individual has experienced, the source of those attacks, and what types of information was lost, stolen, or damaged by the incident. This question must be reworded to clarify that botnets, Distributed Denial of Service (DDoS), and Malware should all be included in a "yes" answer.



VIRUS 31 **[ASK ALL]** ***[COMPUTER VIRUS]***

[Apart from anything you have already mentioned], in that time…has a computer or other internet-enabled device of yours been infected or interfered with, for example by a virus?

DO NOT INCLUDE VIRUSES WHICH WERE BLOCKED BY ANTI VIRUS SOFTWARE BEFORE INFECTING THE DEVICE

INTERVIEWER: IF RESPONDENT MENTIONS RANSOMWARE, BOTNETS, DDoS ATTACKS, MALWARE THEN CODE YES.

1. Yes – ASK **NVIRUS**
2. No – GO TO **PROBES**

This question will be asked followed by a question which establishes relations between singular events collected in previous questions. For example, did the virus attack also result in financial fraud? Unfortunately, due to software limitations, it will not be able to be asked in the same manner as the CSEW questionnaire. Instead, the question will be broken out into multiple individual questions, and each one will be tallied. This is expected to have a minimal impact on final results.

Lastly, a series of similar questions that determine the severity and frequency of related events will be asked, when applicable, to the respondent. These questions establish similarities and relations between events. For example, was the attack from the same person or group of people or did the same virus cause multiple offenses e.g. data loss and theft. It is important to ensure that linked events are captured, which will be accomplished by asking a question that asks if these events are linked. This question will be reworded in such a way that it can be asked individually, and the answers will supersede previous results as the CSEW instructions require the administrator of the test to modify previous answers if necessary.

Chapter 4: Results/Findings

The importance of focusing on the victim of the crime is nothing new, but the highly connected nature of the internet has made it difficult for researchers to have meaningful discussions on victimization inside of the social sphere (Arstanbekov, et. al., 2024) (Button, et. al., 2025). The concept that those enforcing the law could also be the victim of a similar crime, thus contributing to bias in their perceptions of the crime, isn't a far stretch either. Further analysis into victimization and how public safety personnel's personal experience or experience through their capacity as an employee with cybercrime may need to be analyzed in greater detail. Without understanding what, if any, impacts the individual has on a personal level it will be difficult to draw conclusions on the individual's desire to improve skill sets through training to better combat cybercrime for the community.

An area that will likely need exploration outside of this proposed survey is to what level does age impact the views of respondents? Do older generations view attacks that are cyber-enabled or cyber-dependent more or less severe than younger generations? Additionally, what direction are these views trending within the public safety sector should be evaluated to ensure that policy and training are in place to ensure that victims receive the same response regardless of the vector of the crime.

Making this distinction in cyber-dependent and cyber-enabled will help to better understand if it has an impact on how the respondents view cybercrime. If $100.00 is lost through fraud, do respondents see it as equally severe whether that fraud took place in person, or digitally through email? Likewise, if a virus destroys $1,000,000.00 worth of industrial machinery is it considered as severe as an arsonist that destroyed the same machinery? These questions must be explored to better understand how public safety professionals respond to crime with a cyber component.

There is a growing need globally on the importance of cyber education and awareness, which is apparent in Turkey, India, and many states across the US, including Rhode Island. Public- private partnerships into training and awareness of cybercrime have been on the rise. It is argued that these partnerships strengthen the public's understanding, as well as enhancing police officers' knowledge of crimes that would impact the community. These training sessions follow a similar set of goals to educate the public and train their public safety personnel. But they also have the added benefit of tailoring the training to the needs of the community whether it be denial of service attacks on Turkish websites or attacks on critical infrastructure in Rhode Island. (Turkish police to receive cybersecurity training amid surge in cybercrimes, 2019) (Students from 22 states take part in Amroha Police cybersecurity training, 2025) (State police host cybersecurity training sessions., 2018).

With training being an area of focus, it is helpful to remember that, at the core of the matter, members of public safety are employees, and therefore representatives, of the organizations that they work for. The investigation into risk assessment of those employees and their overall perception of cybersecurity has been well examined and findings indicate that the less aware an individual is of technology, the less likely they are to understand the consequences

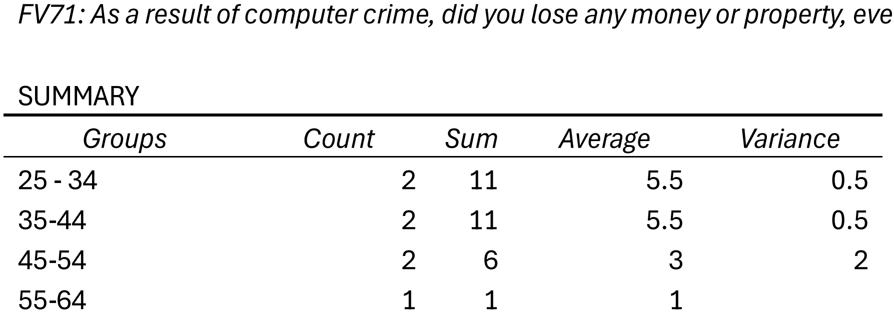
(Hadlington, 2018). A culture of cyber training and awareness is necessary within public safety organizations to prevent these behaviors that would otherwise negatively impact on the community and victims (Alshare, Lane, & Lane, 2018).

An organization's perception of cyber security impacts not just their internal operations, but how they interact with cases involving technology (Whittaker, 2018). Inspector General investigations into vulnerable computer systems at the US Department of Homeland Security, discovered grossly insecure systems which house vital criminal justice data and other highly sensitive data on them. Without a culture of cyber awareness, it is difficult for cybercrime investigators to empathize with victims.

Unfortunately, results were limited to thirty-one respondents across police, fire, and the sheriff's office. Additionally, only 1 respondent from the following age categories: 55-64, 65 and over, and under 25. This limits analysis of potential findings, in attempt to overcome this, some ANOVA calculations will be run with those age groups excluded in order to compare against those findings.

Overall, the findings suggest that there is no statistical correlation between age and the rate at which the respondent's experienced cybercrime on a personal level. P-values for all responses were above 0.05, with the lowest being 0.069 for question "As a result of computer crime, did you lose any money or property, even if you later got it back?" (Figure 1).

Figure 1



FV71: As a result of computer crime, did you lose any money or property, even if you later got it back?

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
25 - 34	2	11	5.5	0.5
35-44	2	11	5.5	0.5
45-54	2	6	3	2
55-64	1	1	1	

65 and over	1	1	1	
Under 25	1	1	1	

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	35.2222222	5	7.04444444	7.04444444	0.06946055	9.01345516
Within Groups	3	3	1			
Total	38.2222222	8				

Given the limited number of responses, this same question was re-run to remove the three age groups that have limited responses raising the p-value to 0.136 (Figure 2), confirming that the respondents age did not create a significant significance in their rate of victimization even within a smaller subset of the groups.

Figure 2

*FV71: As a result of computer crime, did you lose any money or property, even if you later got it back? *Three age groups*

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
25 - 34	2	11	5.5	0.5
35-44	2	11	5.5	0.5
45-54	2	6	3	2

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	8.333333	2	4.166667	4.166667	0.13619	9.552094
Within Groups	3	3	1			
Total	11.33333	5				

Although the overall responses p-values show that no statistical significance between groups exists, the lower p-value for question FV71 when compared against the other questions does suggest that with a larger sample size, a significant result may arise to indicate that loss of money or property may play a factor when discussing differences among the age groups.

Lastly, the highest p-value, found in question FV84 which specifically if individuals were tricked into sending money, indicates that any variation in the groups is simply by chance. Analysis into this exceptionally high p-value could be an avenue for further discussion to determine if having a monetary transaction increases an awareness of a potential crime or scam, regardless of if there is a cyber aspect at play (Figure 3).

Figure 3

FV84: As a result of a computer crime, were you tricked or deceived into sending or transferring money to an individual, company or organization who turned out to be not who they said they were?

SUMMARY

Groups	*Count*	*Sum*	*Average*	*Variance*
25 - 34	2	11	5.5	40.5
35-44	2	11	5.5	40.5
45-54	2	6	3	8
55-64	1	1	1	
65 and over	1	1	1	
Under 25	1	1	1	

ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Between Groups	35.2222222	5	7.04444444	0.23745318	0.92217362	9.01345516
Within Groups	89	3	29.6666666			
Total	124.222222	8				

Lastly, it is important to note that while p-value in figure 1 indicates that variation is by chance, the similar variation within group 1 indicates that there is a similarity in the younger age groups. The 0.5 variance has a low variability between the 25-34 and 35-44 groups in question FV71 and other results in the survey reflect this anomaly. Further analysis into this anomaly is necessary to determine if the effectiveness of training between age groups is a larger factor in understanding new technologies or if the practical application of technologies through training is more important.

Chapter 5: Discussion and Recommendations

A recurring theme in the literature is the need for additional training for law enforcement to combat cyber dependent and cyber enabled crime. The primary reason for this need for training is the ever-changing nature of technology. As quickly as one technology gains adoption by criminals, it is usurped by a similar technology by a different name. The multitude of encrypted communications apps like WhatsApp to Snapchat highlight this, but it is not limited to communications. Financial applications and mobile payment like PayPal, Venmo, CashApp, and Robinhood all add to the complexities of trying to understand or in the case of law enforcement, prevent or prosecute cybercrime. The ease of access to these apps and the conveniences they bring only compound the issue (Button,2025) (Khan, 2024) (Curtis & Oxburgh, 2023).

The findings, while potentially not conclusive, tend to indicate that the training regarding cybercrime between the age groups within public safety officers has been successful. That is to say, successful to the extent that the varying age groups are victimized at an equal rate to each other. While this result may seem counter-intuitive, the multitude of programs to aid law enforcement in getting that training has exploded in recent years. The outreach program by the Secret Service's National Computer Forensics Institute (NCFI), that aids in the training of State, Local, and Tribal law enforcement members, is one of the free programs to assist those officers in becoming better trained and equipped to combat cybercrime (Cyber Investigations, 2025).

This begs the question: have these training investments in public safety been so effective as to eliminate the problems that Button, Khan, and Curtis & Oxburgh postulated? Perhaps, to the extent that training programs have been developed for those technologies that the previously mentioned researchers discussed. However, the rapid change in technology and the development of new technologies effectively wipe out any gains in training as quickly as they are made. Due to the rapid advancement in technology, comprehensive training methods must be continually adapted to ensure they are effective at teaching public safety officers the skills that are needed to cope with emergent technologies (Milojević, S., Milojković, B., & Janković, B., 2025).

While it has already been stated that additional research will be needed into training avenues for public safety personnel to help overcome the rapid change in technologies and how they are used in crime, it can be reasonably concluded that current efforts into the matter are effective. However, there is a near constant barrage of emergent technology that must be evaluated on its own.

These technologies, whether it be faked videos produced by consumer grade Artificial Intelligences like SORA2 which has recently been made available for public use or more mature technologies that have been used in cybercrime for years, require further examination (SJinn Shatters AI Video Limits, Integrating Sora2 and Veo3 for Minute-Long, Character-Consistent Storytelling., 2025). Even more dubious and mature technologies cryptocurrency which is likely one of the largest drivers and enables cybercrime in the modern era with tens of thousands of payments for ransom made daily, and over 100 active known cyber-criminal groups. Cryptocurrency warrants an enormous amount of examination on its own, but in the context of this proposal, how do individuals in public safety view, use, or leverage cryptocurrency (Gomez, van Liebergen, & Caballero, 2023).

There is no shortage of research that is needed to better understand, and train public safety officers on its uses in the context of crime (Milojević, S., Milojković, B., & Janković, B., 2025). However, the challenge lies in how to train the officers. Research into the evolution of police training suggests that non-vendor specific vocational training that focuses on not just theoretical discussion of technologies, but the hands application, is key to an effective training regimen. (Kussainova, Z., Sartbekova, N., & Abakirov, A., 2025). New technologies like Artificial Intelligence must be examined for the new ways in which they can be used to trick or deceive, along with older technologies like cryptocurrency which have matured in their use to be both a conduit for criminal financial transactions and a legitimate currency for worldwide use.

Problem Discussion

Technologies ever evolving nature have given rise to new crimes, and new ways of committing old crimes (Stewart, 2018). This can easily be explored by looking into the evolution of one the most notorious and well-known internet scams, the Nigerian Prince scam (Okosun, 2023). This scam, which has its origins in the Spanish Prisoner scam of the early 1900’s, seeks to advance money from the victim in return for a larger payment once the prince or prisoner is free from bondage. The Nigerian Prince scam gained notoriety by utilizing a new technology, E-mail, to contact victims.

While the underlying crime of fraud and victimization is the same, the technologies used to commit crime are a century apart and could not be fathomed by victims. Public safety officers need to be trained in new and emergent technologies in order to detect, prevent, or otherwise fight crime. Understanding that the underlying crime of fraud taking place is not enough. The officer must also have at least a surface level understanding of the technological mediums that the fraud was committed in. New and emergent technologies, like encrypted chats, Artificial Intelligence (AI), and Digital Currencies such as Bitcoin, place a new spin on old crimes and create new avenues for attacks. It is imperative that officers know of these technologies' existence and have a rudimentary understanding of their capabilities to detect when a crime has taken place (Warner, 2021).

The recent rapid advancements in Artificial Intelligence with OpenAI's deployment of SORA2 has given the ability to anyone with a computer or smart phone to create realistic videos with audio. Additionally, story consistent avatars can be inserted into the video (SJinn Shatters AI Video Limits, Integrating Sora2 and Veo3 for Minute-Long, Character-Consistent Storytelling., 2025). While this technology is merely weeks old at this time, the implications of being able to fabricate security camera, smartphone footage, or even body worn camera videos are severe. This capability of the average person being able to create believable falsified video evidence, along with an officer that is unaware that the technology to create that video even exists is a recipe for disaster.

Theoretical Discussion

Part of the challenge for public safety personnel is the ability to determine the differences and significance of a cyber-related crime and a cyber-dependent crime. Researchers have questioned the nature of the attack and the perceived severity which ultimately impacts the victimization of the individual by the response (or lack thereof) of law enforcement (Arstanbekov, et. al., 2024) (Button, et. al., 2025). They go on to postulate if cyber-dependent crimes, due to their technical nature, receive less focus than a more tangible crime that simply leverages cyber and technologies to execute a more traditional crime.

Efforts to create communications channels for local officials to tap into much needed federal resources are often expensive, but new initiatives are underway to improve communications. Facilities offering statewide access for local law enforcement officers to utilize the expertise and federal cybercrime units are being built. In Fresno, the California Cyber Crime Center was constructed to aid local law enforcement by providing eCrime forensic services of the Department of Justice to local law enforcement efforts (Ellis, 2016). The facility houses cyber experts, and specialized equipment necessary to analyze cellphones and other digital evidence for local law enforcement that lack the skills or equipment to adequately investigate.

While other countries have recognized the problem of lack of qualified public safety officers to investigate and respond to cybercrime, the responses to this issue are as diverse as the countries. Poland has responded by creating specialized bureaus and task forces, such as the Central Cybercrime Bureau (CCB), specifically to combat cybercrime, recognizing that Polish police officers were not equipped or trained to combat the proliferation of new cyber-attacks (Marta, 2024). Singapore has recognized that much cybercrime originates outside of its jurisdictions. The response is to fundamentally change policing efforts from prosecution of criminals to prevention and education policies (Khan, 2024). Turkey and India are instituting combined training efforts with police and citizens to increase awareness and strategic communications about cybercrime as it impacts local communities (Turkish police to receive cybersecurity training amid surge in cybercrimes, 2019) (Students from 22 states take part in Amroha Police cybersecurity training, 2025).

Organizations from all business sectors have realized that their employees are often the target of attack in cybercrimes. In the words of Snell (2019), “the human element” is the weakest link in any organization and organizations take a “set it and forget it approach” to cyber security and instances of cybercrime with limited access to training resources. In the case of public safety, it becomes apparent that this approach is not optimum. How can an officer protect members of the public from a crime when the officer does not understand the crime or cannot describe the details of the crime?

The global nature of cybercrime means many of the offenses go unprosecuted, or even unreported by victims, some attribute this to the aforementioned lack of expertise, awareness, and training for police officers (Button, et. al., 2025). The perception is that a crime that is cyber in nature is less important than that of a similar crime that is physical or more tangible in nature. The issue of globalization is further compounded by the relatively new nature of cybercrime (Arstanbekov, et. al., 2024). This has put pressure on public perception and law enforcement frameworks to deal with the issue. Whether the larger issue lies with the criminal justice system or the public perception of the crime, it is necessary to understand the perception and capabilities of public safety personnel that are on the front lines. Those frontliners know the capabilities of the public safety agency, the community members, and the types of cybercrimes affecting their community. Understanding the perspectives of public safety personnel and their relative technological expertise will help them to better realize long term solutions to the issue at hand by looking at various age groups within the public safety sector and analyzing the rate that they have personally experienced cybercrime.

The following six age groups have been chosen, under 25, 25-34, 35-44, 45-54, 55-64, and over 65 to evaluate the rate at which each age group experiences various types of cybercrime. The perception of cybercrime for police officers is heavily influenced by age and the experiences the individual officer had with those crimes (Hadlington, et. al., 2021). How are officers within these age groups impacted on a personal level by cybercrime? Does age affect the rate at which they are impacted and to what degree?

Button et. al. largely attributes instances of fraud and cyber dependent crimes increase in quantity following COVID-19. This increase in occurrence also fueled public perception that the severity of any individual cybercrime had gotten worse as well. However, the fact still remains that cyber related and cyber-enabled crime is increasing and displacing more traditional crimes. To further combat this, an evaluation into the perception of cybercrime from the crimefighters perspective is necessary to determine to what degree those crime fighters can detect and therefore combat crime that has a cyber component.

Chapter 6: Conclusion

How a person understands technology can greatly influence how they perceive cybercrime. When that individual is in public safety, it also affects how they fight cyber-crime for the community. With the constant advances in technology ways to commit crime are constantly evolving. The need for a public safety officer to understand these technologies is paramount to ensure they can adequately combat crime. In doing so, we must seek to understand how do public safety officers perceive the severities of cybercrime, and do their experiences change their understanding with age?

Although this research saw interesting anomalies like the low variations between the age groups bear further research, in the end, personal victimization has no bearing on perceptions of cybercrime. Age groups saw similar levels of personal experiences with cybercrime, with only minor variations on specific types of fraud. Concerns from the research, such as low sample size, require further evaluation and larger sampling to ensure accuracy.

It is important to keep in mind the human element when a public safety officer is also a victim. Will our public safety partners report accurately their own experiences with cybercrime, particularly if it makes them look foolish? Members of public safety may be victims of cybercrime that goes unreported for fear of embarrassment or even reprisal from management. It is often overlooked that police can be victims as well. Examination into the victimization aspect for public safety personnel is needed to evaluate this as a concern. To what degree does this victimization affect their daily work and prosecution of cyber related crimes? Does their own victimization make the individual more assertive in their fight against cybercrime, or does it cause them to be more protracted because they feel inadequate for not understanding? Where does this lack of understanding stem from, and can it be fixed with additional and regular training?

Cyber crime's international nature makes it difficult for local members of public safety to combat. Prosecution is difficult, if not impossible in many cases. However, awareness through training, not just to police but to members of the community aids in prevention. But it cannot stop there, public safety needs to be able to act and react to cybercrime that endangers the community as a whole. A computer compromised with ransomware could shut down a water treatment plant and endanger the entire community. Police, Fire, EMS all must be able to work together not just to stop these threats from materializing, but to address them when they do. This cannot be done without adequate training and awareness of these attacks and how they could impact the community.

Overcoming these built-in assumptions about how crimes are perpetrated to train public safety officers is necessary. Further research focusing on specific types of cybercrime and the training that they should receive would be a benefit to public safety and the public at large.

Determining if an awareness of a new technology is enough to aid in the prevention, detection, or prosecution of a cybercrime is enough to reduce the overall occurrence of said crime, or must advanced and detailed training take place in order to accomplish this?

The road to answering this question may not have a clearly defined path, it is necessary to evaluate it to determine the effectiveness of training. As previously discussed, the idea of ever evolving training regimens is nothing new, whether it is through local channels, federal, or even internationally, cyber training for public safety officers is a near constant task (Turkish police to receive cybersecurity training amid surge in cybercrimes, 2019) (Students from 22 states take part in Amroha Police cybersecurity training, 2025) (State police host cybersecurity training sessions., 2018). With this in mind, shifting to an evaluation mindset of ensuring the update of those trainings, and the evaluation of the materials being covered should be considered. With that said, this evaluation of the training, along with updates to the training to include new and emergent technologies in critical to ensure that officers are prepared in their efforts of protecting the public, thus ensuring the ability of public safety officers to effectively combat crime.

References:

Alshare, K., Lane, M., & Lane, P. (2018). Information security policy compliance: a higher education case study. Information and Computer Security, 26(1), 91-108.

Arstanbekov, M., Seidakmatov, N., Tatenov, M., Kanybekova, B., & Kakeshov, B. (2024). Victimological aspects of countering internet crime: State and local government practices. Social & Legal Studios / Socìalʹno-Pravovì Studìï, 7(1), 221–234. https://doi.org/10.32518/sals1.2024.221

Biden Signs Cybersecurity Executive Order Following Colonial Pipeline Hack. (2021). All Things Considered.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2025). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. Criminology & Criminal Justice: An International Journal, 25(2), 670–691. https://doi.org/10.1177/17488958221128128

News | cisa. (2025). https://www.cisa.gov/

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in "real world" policing and law enforcement. Police Journal, 96(4), 573–592. https://doi.org/10.1177/0032258X221107584

Gioia, G., & Lener, S. M. (2024). The Protection of Individuals against Privacy-Invasive and Discriminatory Inferences under European Law: From the General Data Protection Regulation and the Digital Content and Services Directive to the Artificial Intelligence Act. Collected Papers of Zagreb Law Faculty / Zbornik Pravnog Fakulteta u Zagrebu, 74(5/6), 861–880. https://doi.org/10.3935/zpfz.74.56.6

Glenn, A. (n.d.). Equifax: Anatomy of a Security Breach. Georgia Southern Commons.

Gomez, G., van Liebergen, K., & Caballero, J. (2023). Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage.

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems,* 33(1)*,* 296–325. Retrieved from https://doi.org/10.1080/07421222.2016.1172440

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology, 269–281. https://doi.org/10.5281/zenodo.1467909

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2021). A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime. Policing: A Journal of Policy & Practice, 15(1), 34–43. https://doi.org/10.1093/police/pay090

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science, 8(1), 1. Retrieved from https://doi.org/10.1186/s40163-019-0097-9

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore †. Laws (2075-471X), 13(4), 44. https://doi.org/10.3390/laws13040044

John Ellis. (2016, October 11). Attorney General Harris launches cyber crime initiative in Fresno stop; * In a visit to the state crime lab at Fresno State, Kamala Harris announces the California Cyber Crime Center, also called C4. It will offer digital forensics and cyber security expertise to law agencies statewide. Fresno Bee, The (CA).

Kamuda, D. (2018). Wybrane zagadnienia z zakresu cyberprzestępczości[In:] Golonka, A., Trybus, M., ed., Prawo karne w obliczu zmian i aktualnych problemów polityki kryminalnej. Rzeszów: Wydawnictwo UR

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review,* 13(1)*,* 10–21. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=122028355&site=eds-live&scope=site

Kussainova, Z., Sartbekova, N., & Abakirov, A. (2025). Essential Characteristics of the Process of Modelling Educational Programmes of Pedagogical Directions in Technical and Vocational Education. Journal of Vasyl Stefanyk Precarpathian National University, 12(3), 150–168. https://doi.org/10.15330/jpnu.12.3.150-168

Marta POMYKAŁA. (2024). The Central Cybercrime Bureau as a New Police Service Established to Combat Cybercrime. Humanities and Social Sciences, 31(2), 131–141. https://doi.org/10.7862/rz.2024.hss.24

Matt Warner. (2021, September 14). New police boss' experience in technology sector will help fight cybercrime in North Wales. Leader, The - Wrexham Edition (Wales).

Milojević, S., Milojković, B., & Janković, B. (2025). The Effectiveness of Police Forces Through Centuries: The Evolution of Training Process in Contemporary Social Context. NBP - Journal of Criminalistics & Law, 30(2), 127–147. https://doi.org/10.5937/nabepo30-50861

Mollborn, S., Fomby, P., Goode, J. A., & Modile, A. (2021). A life course framework for understanding digital technology use in the transition to adulthood. Advances in Life Course Research, 47. https://doi.org/10.1016/j.alcr.2020.100379

Office for National Statistics (2018). 2017-18 Crime Survey for England and Wales Questionnaire. TNS UK Limited. https://doi.org/10.5255/UKDA-SN-8703-1

Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. Journal of Financial Crime, 30(6), 1653–1663. https://doi.org/10.1108/JFC-08-2022-0185

Russia renews big attacks on Ukrainian power grid using better intelligence and new tactics. (2024). In AP English Worldstream - English. Associated Press.

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. Journal of Management Information Systems, 34(4), 1023–1053. https://doi.org/10.1080/07421222.2017.1394049

Cyber investigations. (2025). https://www.secretservice.gov/investigations/cyber

SJinn Shatters AI Video Limits, Integrating Sora2 and Veo3 for Minute-Long, Character-Consistent Storytelling. (2025). PR Newswire US.

Snell, R. (2019). As Technology Becomes Increasingly Complex, So Must Our Efforts to Combat Its Inherent Security Risks. Journal of Health Care Compliance, 21(2), 29–66.

Snell, L. (2019). Who Is Really Responsible for Cloud Security? PC Quest, 32(7), 58–59. State police host cybersecurity training sessions. (2018, November 23). Associated Press State Wire: Rhode Island (RI).

Stewart, J. M. (2018). (Isc)² Cissp: certified information systems security professional. Hoboken, NJ: Sybex

Students from 22 states take part in Amroha Police cybersecurity training. (2025, June 27). Times of India, The (Mumbai, India).

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Taylor, R. W., Fritsch, E. J., Liederbach, J. R., Saylor, M. R., & Tafoya, W. L. (2023). Cyber Crime and Cyber Terrorism (5th ed.). Pearson Education (US). https://reader.yuzu.com/books/9780137953271

Turkish police to receive cybersecurity training amid surge in cyber crimes. (2019, April 5). Cyber Security Monitor Worldwide (Amman, Jordan).

Vanlyssel, J. (2025). Securing U.S. Critical Infrastructure: Lessons from Stuxnet and the Ukraine Power Grid Attacks.

Whittaker, Z. (2018, March 7). Homeland Security's own IT security is a hot mess, watchdog finds. Retrieved from https://www.zdnet.com/article/homeland-security-cybersecurity-is-a-hot-mess-watchdog-report/