
# CYBER-INVESTIGATIVE EXPERTISE AND TRAINING SURVEY

MICHIGAN STATE UNIVERSITY | School of Criminal Justice

# CYBER-INVESTIGATIVE EXPERTISE AND TRAINING SURVEY

**Jeremiah Schutter**

**Dr. Jeff Rojek**

**Dr. Rachel McNealey**

**Dr. Tom Holt**

**School of Criminal Justice**

**Michigan State University**

**May 2025**

## BACKGROUND

The rise of computers and the Internet in the 1980s and 1990s created opportunities for various traditional crimes to move into online spaces, such as fraud schemes, sexual offenses, and stalking and harassment behaviors. Additionally, the growth of online commerce and sensitive data storage created opportunities for new forms of crime, such as computer hacking to harm data and protected systems.

The novelty of these offenses, the unique evidentiary issues they present, and the complexities of investigation across jurisdictional boundaries make cybercrimes exceedingly difficult to pursue for state and local police agencies. Policy makers and policing scholars have made recommendations to improve the cybercrime response capacities of local police agencies since the early 2000s (e.g. Goodison et al., 2019; Stambaugh et al., 2001). The guidance has remained relatively stable over time: 1) greater investments in technological resources, 2) increasing training for officers and detectives, 3) increased training for police management, 4) improved counting of cybercrimes in official statistics to document the scope of the problem, and 5) improved public awareness of the problem.

Criminal justice research has found that the capacities of local agencies are increasing, but with distinct differences depending on location (Moloney et al., 2022). Evidence suggests that local agencies in major US cities are more likely to have specialized task forces to respond to cybercrime (e.g. Willits & Nowacki, 2016). Local agencies are also less likely to investigate computer hacking and malware cases compared to crimes involving child sexual exploitation and stalking (e.g. Bossler & Holt, 2012; Holt et al., 2015).

Though beneficial, there have been few national assessments of police agencies' responses to cybercrime in the last two decades (e.g. Holt et al., 2010; Moloney et al. 2022). The difficulties in surveying this population, coupled with a seemingly low number of cybercrime policing researchers may account for these gaps (Holt et al., 2015). Regardless, there is a need to explore the extent to which local agencies are aware of cybercrimes, and their overall resources and allocations to digital forensic and cybercrime investigation. This study attempted to address this gap through a national survey of state, local, and tribal law enforcement agencies.

## DATA COLLECTION

The survey was administered to a national sample of agencies of local law enforcement, municipal police department and county sheriff/police departments. The research team initially drew a stratified random sample of 1,000 agencies using the National Directory of Law Enforcement Agencies (NDLEA), which once cleaned (e.g. duplicate entries, missing data) represented a sampling frame 14,368 city and county law enforcement agencies. In order to have representation by agency size, the agencies in the NDLEA were separated in four size strata (1-

19 officers, 20-49 officers, 50-99 officers, and 100 or mor officers) and then 250 agencies were randomly selected from each strata. The survey was conducted in conjunction with the Center for Cybercrime and Investigation Training at Michigan State University. In light of center training interests, an additional random sample of 157 of Michigan agencies not selected in the initial national sample was also drawn.

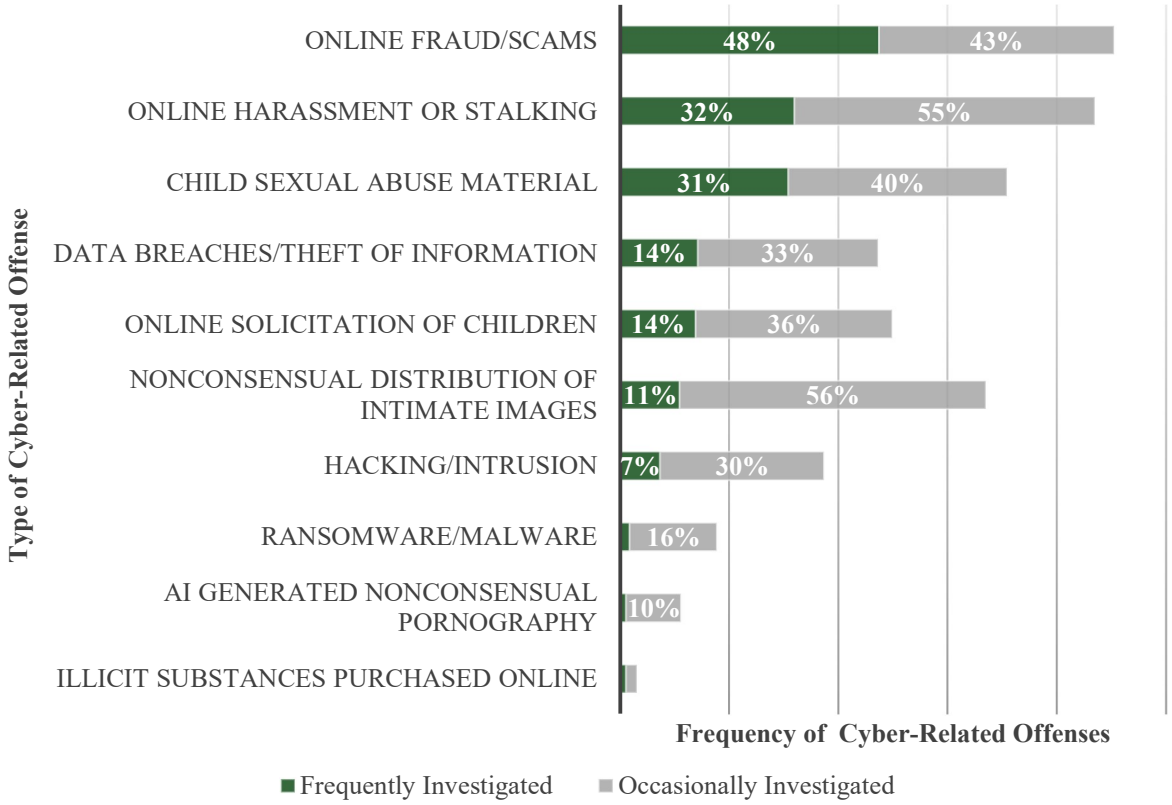
Surveys were mailed to the selected agencies, with the opportunity to respond with the mailed hard copy or answer through a secure online survey site. A total of 338 agencies responded to the survey, representing a 29% response rate. When broken down by the original national data collection and supplementary Michigan data collection, there were 256 (26% response rate) and 82 (56% response rate) agencies responding respectively.

## AGENCY DIGITAL INVESTIGATIVE EXPERIENCES

### Frequency of Investigations into Cyber-Related Offenses in the Past 12 Months

The agencies were initially asked to provide information regarding the frequency of investigations into cyber related offenses in the past 12 months, with the option to report they never, rarely, occasionally or frequently investigate the given offense. Figure 1 shows that fraud/scams (48%) and harassment/stalking (32%) were the most investigated crimes whether looking just at those who reported they frequently investigator (48% and 32% respectively) or looking at frequently or occasionally investigated combined. Child sexual abuse material and nonconsensual distribution of intimate images where the next most like offenses to frequently or occasionally be investigator by the agencies, though child sexual abuse material was more likely to be frequently investigated (31%). Illicit substances purchased online and AI generated nonconsensual pornography were the crimes least investigated.

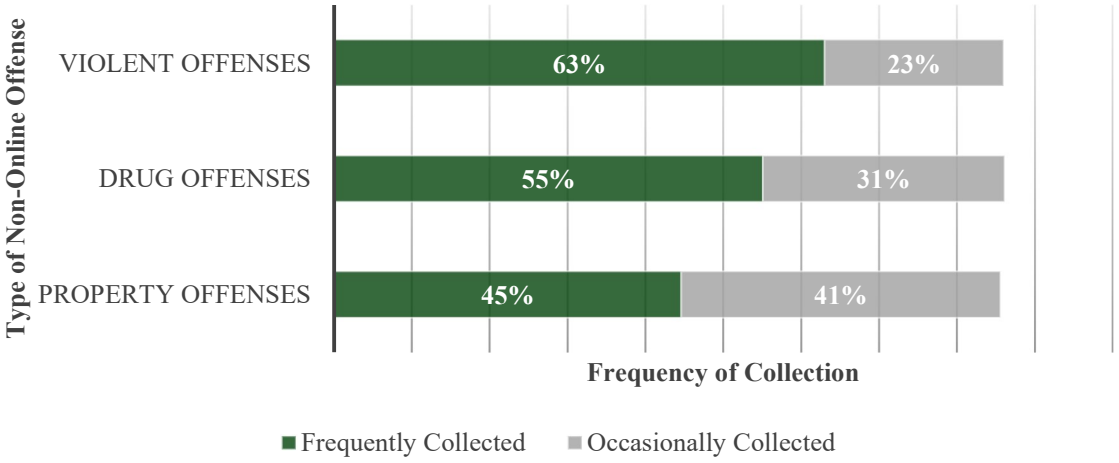
**Figure 1.** Frequency of Investigations into Cyber-Related Offenses




**Frequency of Collecting Digital Evidence when Investigating Non-online Offenses**

Agencies were asked to provide information regarding how often investigators collected digital evidence when investigating non-online offenses. Figure 2 highlights the responding agencies were highly likely to report they collect digital evidence for violent, drug and property offenses, with 86% reporting they frequently or occasionally collect this evidence for each of these categories. Narrowing the focus to how many agencies frequently collect digital evidence for non-online offenses,63% of agencies reported for violent offenses, 55% for drug offenses, and 45% for property offenses.

**Figure** 2. Frequency of Digital Evidence Collection in Non-Online Offenses

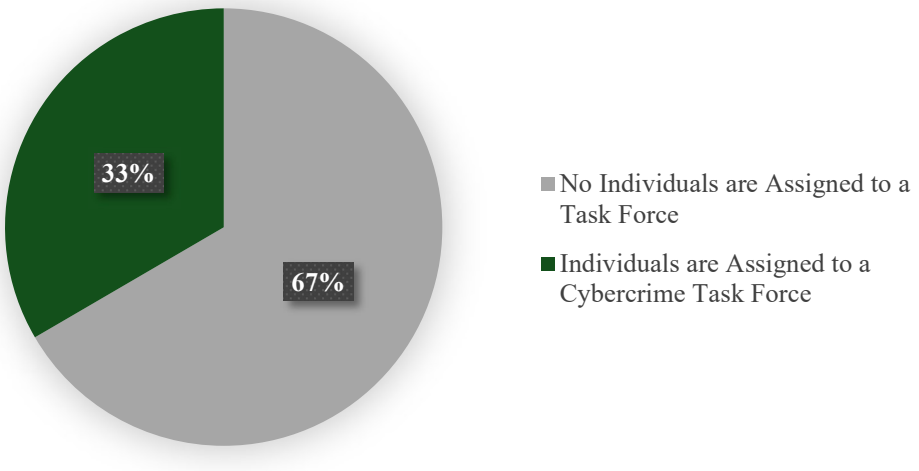



## CYBER-INVESTIGATION CAPACITY

### Participation in Cybercrime Task Force

Agencies were asked if they have personnel participating in a local, state or federal task force dedicated to investigating cybercrime or crimes with digital evidence. Figure 3 presents the result, indicating that 67% of agencies did not have individuals participating in a task force and while 33% did not.

**Figure 3.** Participation Cybercrime and Digital Evidence Task Force

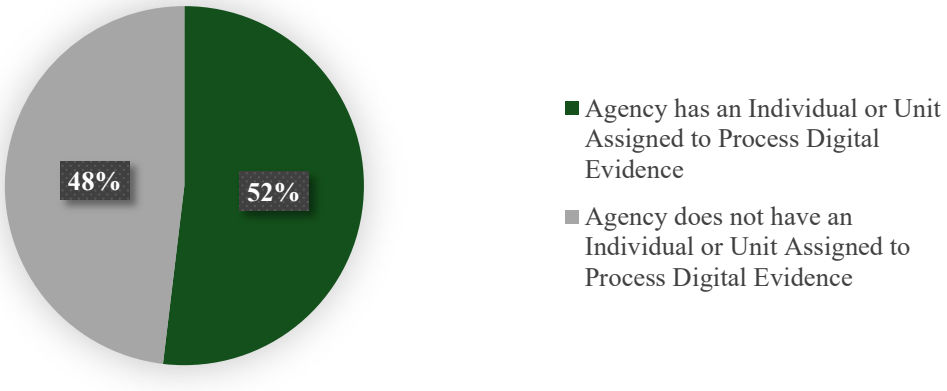



Agencies who indicated that individuals are assigned to a cybercrime task force were subsequently asked the type of task force involvement. Participation only in a local or state task was most likely (44%), followed by only federal task force involvement (36%). Further, 20% of respondents reported that personnel were assigned to local, state, and federal task forces.

**Processing Digital Evidence**

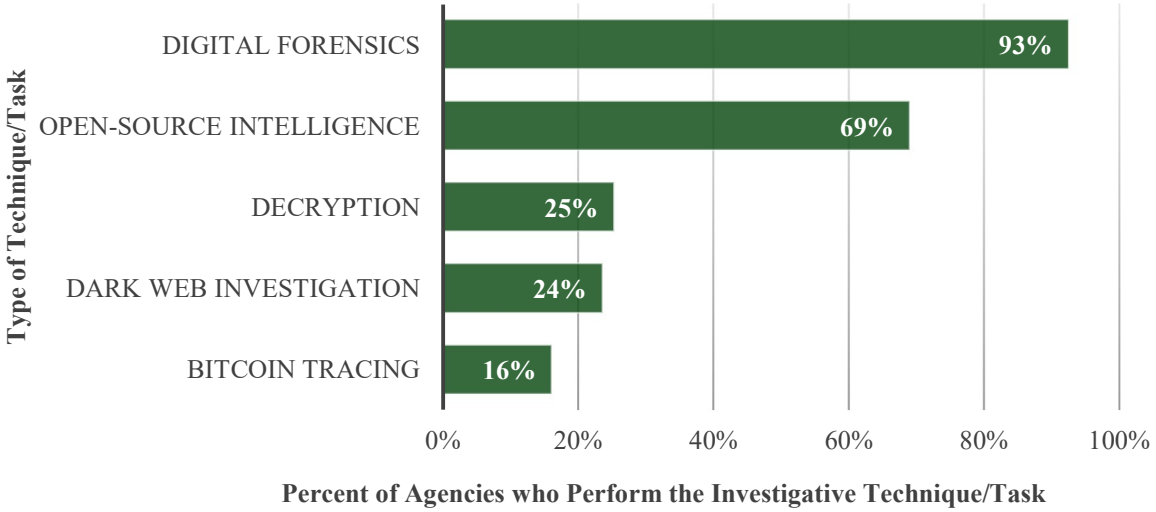
Agencies were asked whether the they had an individual or unit assigned to process digital evidence within the agency. Figure 3 illustrates that the slight majority, at 52% reported having individuals or a unit to manage digital evidence processing and the remaining 48% of agencies reported they do not have this capacity.

**Figure 4.** Assignment of Individuals or Units for Digital Evidence Processing in Agencies



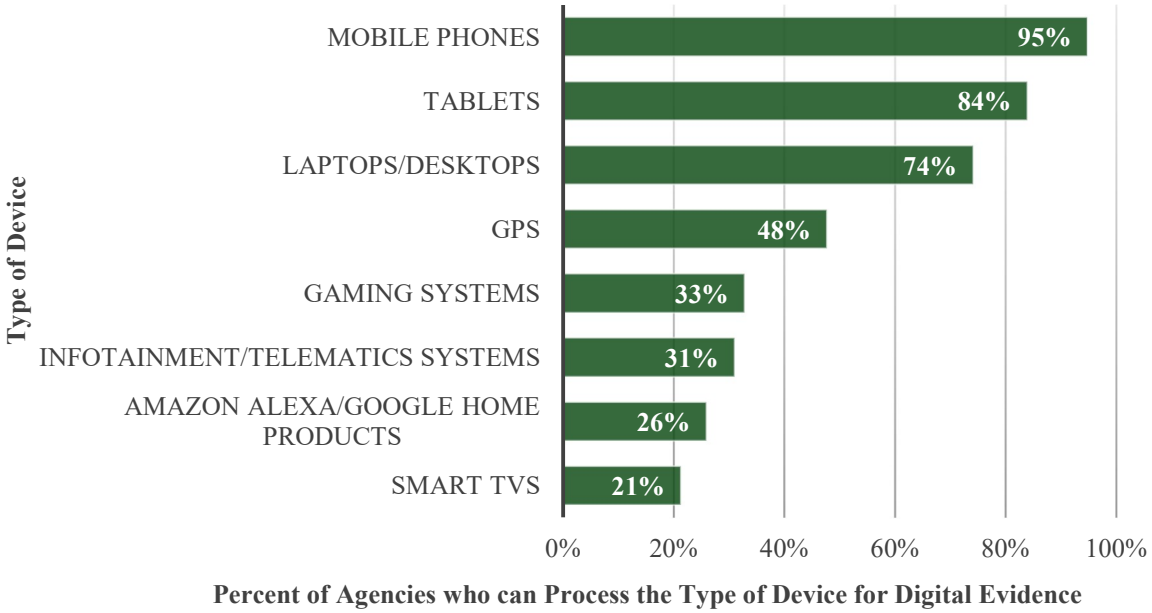

Agencies who indicated that they had personnel assigned to process digital evidence were asked what investigative techniques or tasks they can perform. Figure 4a illustrates that digital forensics was the most common capacity (93%). Open source was the second most common (69%) within agencies digital evidence capacity, followed by decryption (25%) and dark web investigation (24%). Bitcoin trading had the lowest response, with only 16% of agencies reporting that they perform this task.

**Figure 4a.** Investigative Techniques/Tasks Performed by Agency Personnel



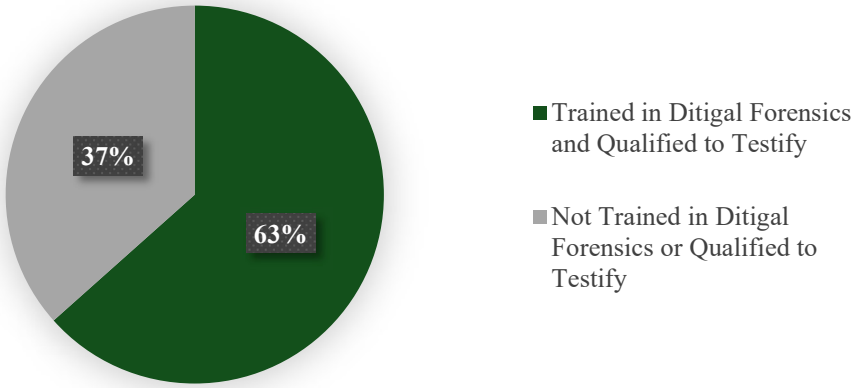
Agencies who indicated that they had personnel assigned to process digital evidence were also asked if personnel could process different types of devices for digital evidence. The most common capability reported by agencies was the ability to process mobile phones, with 95% of agencies reporting this capability as shown in figure 4b. The second and third most common capabilities were processing tables (84%) and laptops (74%). In contrast, agencies were least likely to report the capability to process smart TVs (21%) for digital evidence.

**Figure 4b.** Personnel Capability to Process Devices for Digital Evidence




Agencies with personnel assigned to process digital evidence were also asked whether the personnel received training in digital forensics that would qualify them to testify as a court expert. Figure 4c shows that 63% of agencies reported that their personnel were qualified to testify.

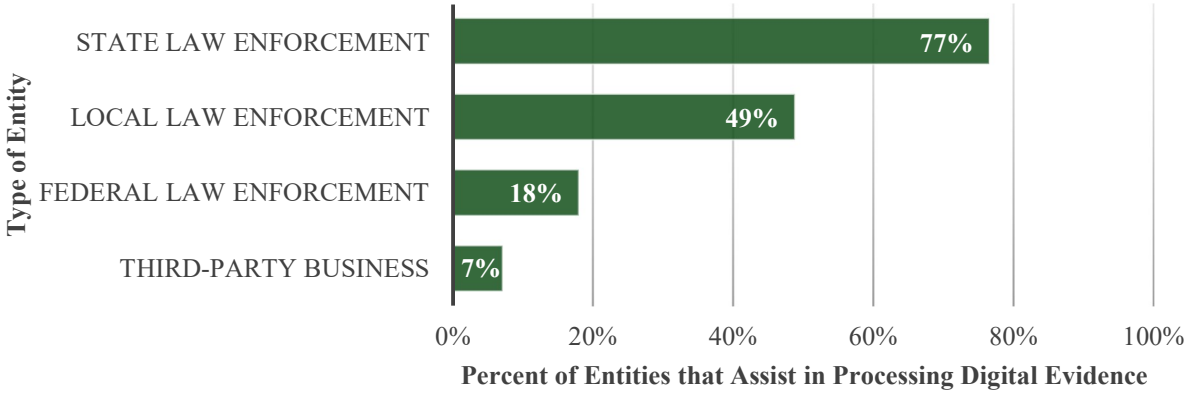
**Figure 4c.** Employee Training in Digital Forensics for Court Expert Qualification



**Assistance in Processing Digital Evidence**

Agencies were asked whether they had a different agency to assist in processing digital evidence that they collected. Figure 5 shows that agencies were most likely to receive assistance from a state law enforcement agency for digital evidence processing (77%), followed by local law enforcement agencies (49%), federal law enforcement (18%), and third party businesses (7%).

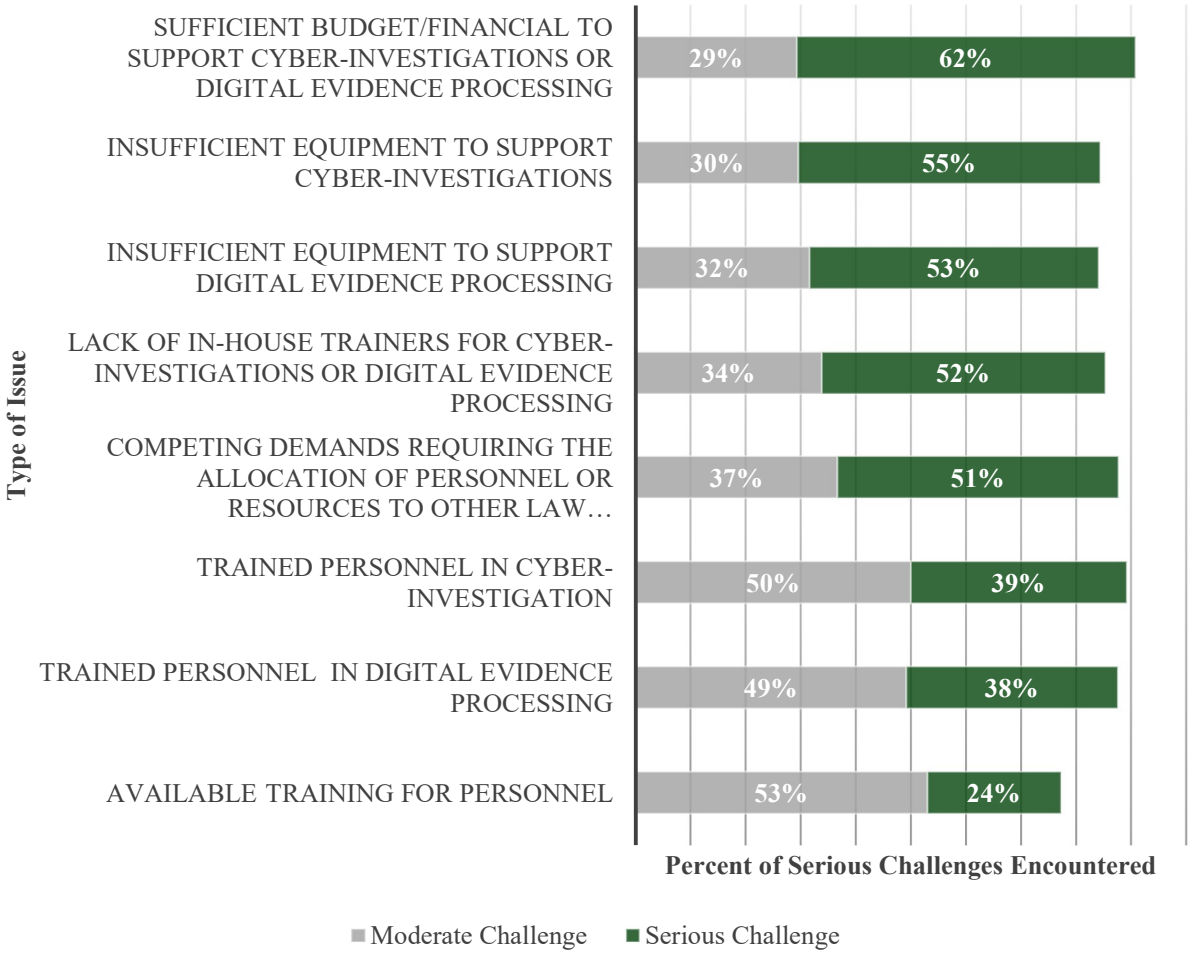
**Figure 5.** Usage of Entities for Assisting in Digital Evidence Processing by Agencies




**Challenges Encountered in Investigating Cybercrimes of Crimes with Digital Evidence**

Agencies were asked to provide insight on challenges encountered in investigating cybercrimes or crimes with digital evidence. Figure 6 provides the results of responses that indicate a moderate or serious challenge. Focusing on where agencies reported they face a serious challenge, having a sufficient budget (62%) was the most significant issue. Insufficient equipment to support cyber-investigations (55%), and digital evidence processing (53%) are the second and third most reported challenges. The availability of training for personnel was least likely to be reported as a serious challenge (24%).

**Figure 6.** Challenges Encountered in Investigating Cybercrimes or Crimes with Digital Evidence

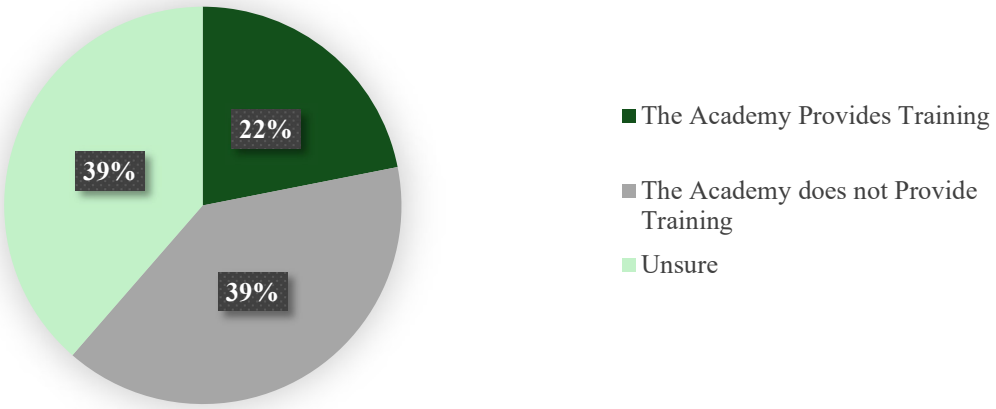


## CYBER-INVESTIGATION TRAINING

### Training Received in the Academy

Respondents were asked if officers received training in their academy in digital investigation techniques and/or cybercrime offenses. Recognizing that many agencies do not operate the academy their officers attend and thereby may not be aware of the training provided in detail, the option of unsure was also provided. Figure 7 shows that agencies are more likely report the academy their officers attend does not provide training on digital investigation techniques and cybercrime (39%) than report their officers do (22%). However, 39% of agencies reported they unsure if officers received this training.

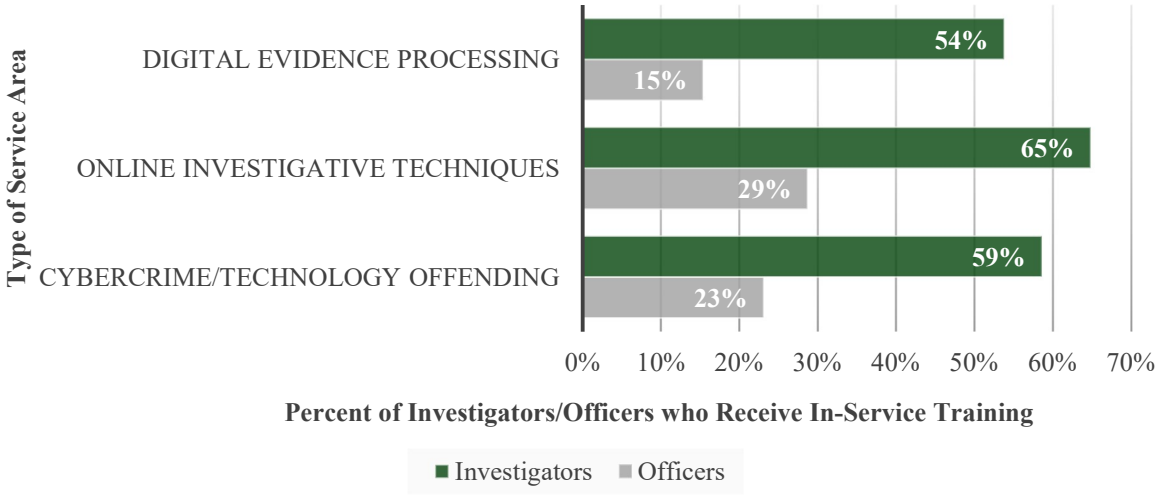
**Figure 7.** Training in Digital Investigation Techniques and Cybercrime Offense in the Academy




### Officer and Investigator Receipt of In-Service Training

Agencies were subsequently asked if officers or investigators in their agency receive any in-service training on different element of cybercrime and related investigations, being asked to separately report for officers and investigators. As shown in Figure 8, 65% of agencies reported their investigators receive training for online investigative techniques (65%). In addition, 59% reported their investigators receive training cybercrime and technology offending 54% for digital evidence processing. Providing this training for officers was considerable lower. Across the responding agencies, 29% reported they provide in-service training online investigative techniques 29% for their officers, followed by cybercrime technology and offending (23%) and digital evidence processing (15%).

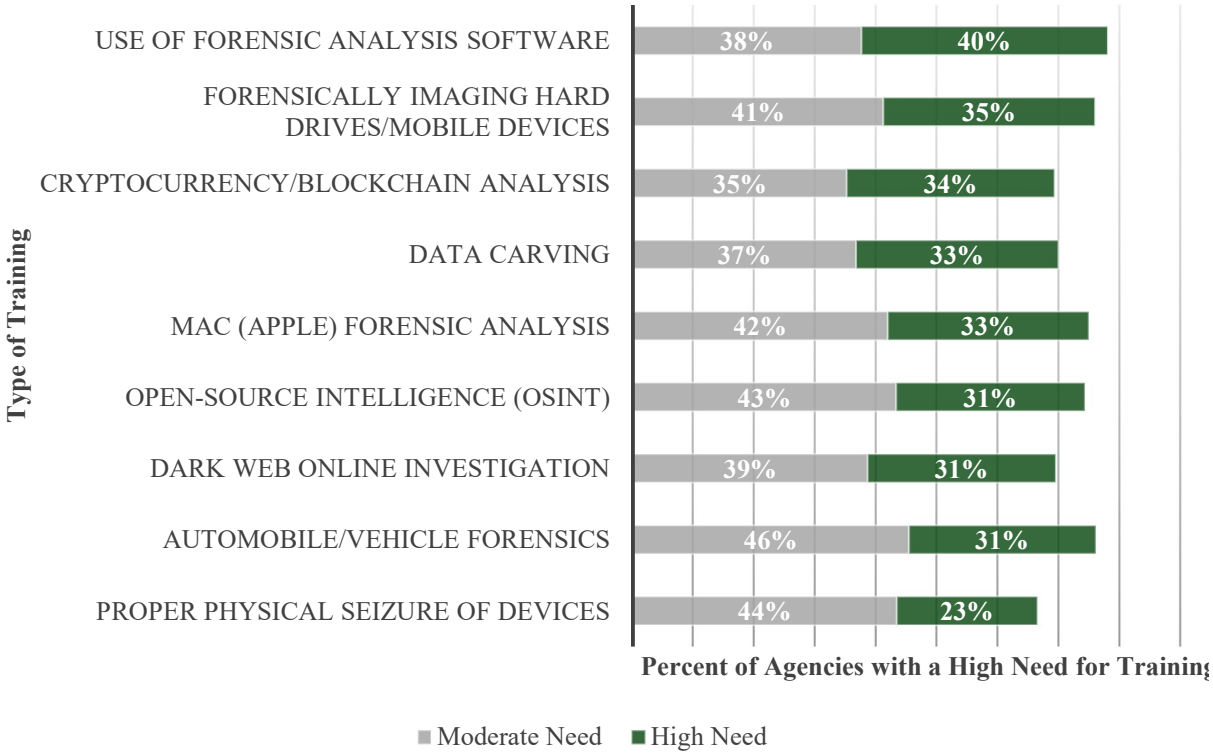
**Figure 8.** In-Service Training for Officers and Investigators in Specific Areas




**Need for Training**

Agencies were asked to indicate the level of need for training in different online investigative and digital evidence processing areas. Overall, 70% or more of the agencies reported they have a moderate or high need for each of the listed training areas. As shown in Figure 9, when focusing on areas of reported high need, 40% reported forensic analysis software and35% for Forensically imaging hard drives. Alternatively, only 23% reported a high need for training on physical seizure of devices (23%).

**Figure 9.** Need for Training in Online Investigation and Digital Evidence Processing

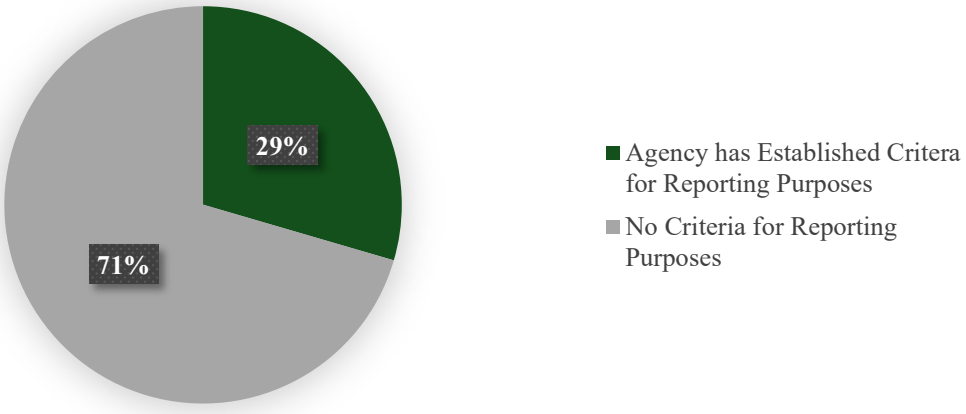



## NATIONAL INCIDENT-BASED REPORTING SYSTEM

### Criteria for Classifying Crime for Reporting Purposes

Agencies were asked if they have criteria for classifying "cybercrime" and/or "cyber-enabled crime" to guide reporting. Figure 10 shows that 71% of agencies had no criteria.

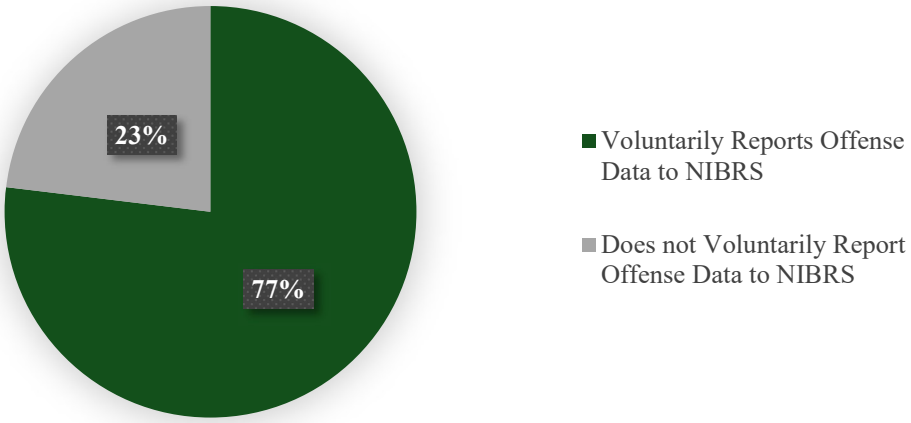
**Figure 10.** Criteria for Classifying "Cybercrime" and "Cyber-Enabled Crime" in Reporting



**Reporting Offense Data to NIBRS**

Agencies were asked if they voluntarily reported offense data to NIBRS. Figure 11 shows that 77% of agencies voluntarily reported offence data to NIBRS. In addition, NIBRS provides the capability for agencies to indicate whether a computer was the object of the reported crime and to indicate whether the offenders used computer equipment to perpetrate a crime. Among the agencies that voluntarily Among the agencies who voluntarily report to NIBRS ,84% of agencies stated they report this computer use information.

**Figure 11.** Voluntary Reporting of Offense Data to NIBRS by Agencies

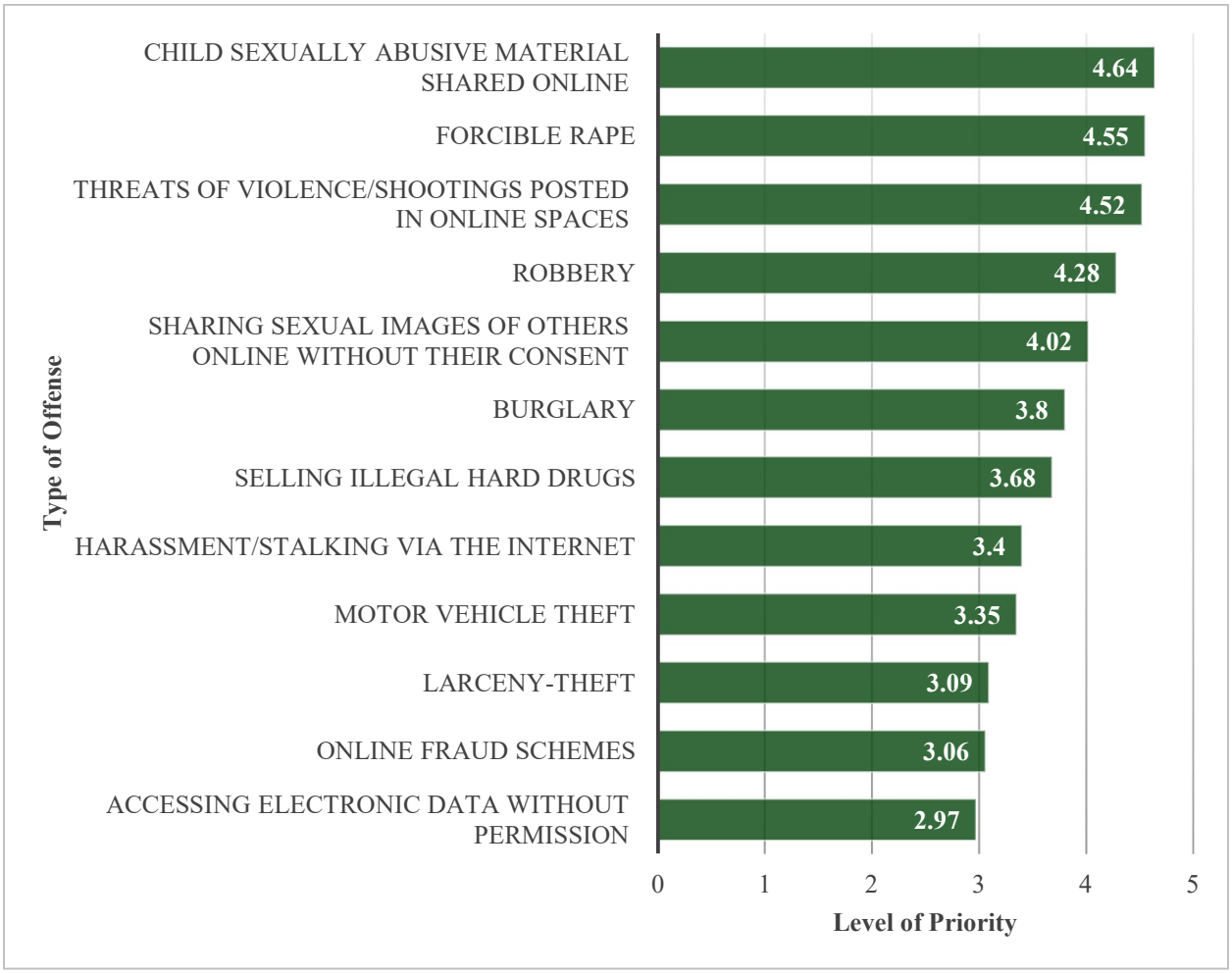



## PERSPECTIVE ON CYBER OFFENSES

**Seriousness of Offense from an Agency Perspective**

The final section of the survey asked the agency respondents their general perspective on cybercrime. – Agencies face a number of demands on limited resources which can shape how they have to relatively prioritize their focus. Among the number of influences this can include amount and nature of criminal activity in your jurisdiction, along with the expectations of community members and elected officials. Agencies were first asked to prioritize a list of crimes, which included cyber-based and non-cyber offenses. The intent is to understand how cybercrimes are viewed as a priority to address in their jurisdiction relative to other non-cybercrimes. Each offense can be rated from 1 (lowest priority) to 5 (highest priority). Figure 12 shows that child sexually abusive material shared online had the highest prioritization across the responding agencies, with an mean score of 4.64 out of 5. Forcible rape was the second most serious, with a mean score of 4.55 out of 5. In contrast, accessing someone else's data without permission was considered the had the lowest mean priority score of 2.97 out of 5. Overall, the scores show some cybercrimes viewed as high a priority to address as serious non-cyber offenses such as forcible rape and robbery.

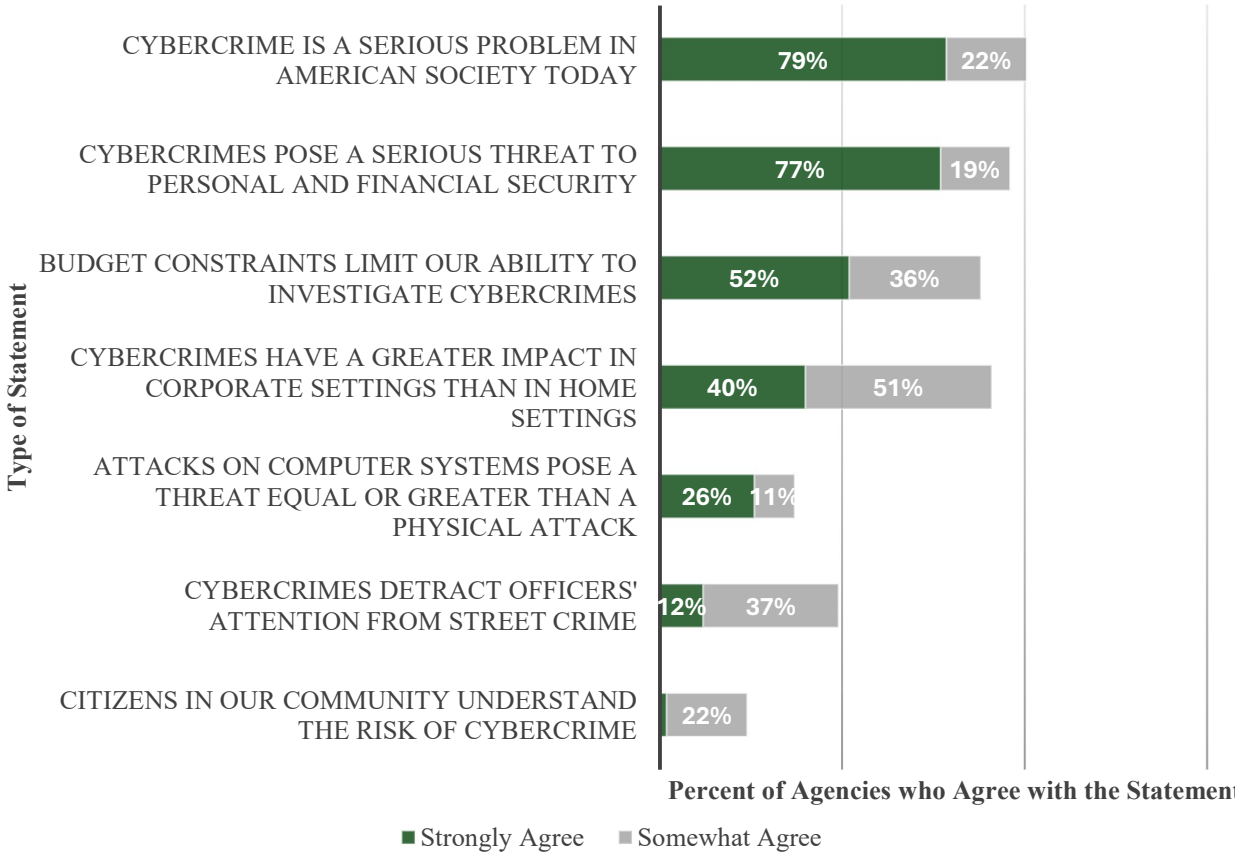
**Figure 12.** Average Priority Level for Different Types of Offenses




**General Viewpoints related to Cybercrimes**

The final question set asked the agency respondent to rank on a four-point scale (strongly disagree, somewhat disagree, somewhat agree, strongly disagree) a series of statements related to cybercrime. Figure 13 shows that 79% strongly agree that cybercrime is a serious problem in American society today and 77% strongly agree that cybercrimes pose a serious threat to personal and financial security. Alternatively, only 1% of agencies strongly agree that citizens in the community understand the risk of cybercrime.

**Figure 13.** General Viewpoints Related to Cybercrimes Relative to Other Considerations




## Summary of Findings and Conclusion

The data from our survey show that a majority of agencies perform digital forensic investigations and can process the most common types of digital devices including mobile phones, tablets, and laptops or desktops. Most agencies have an employee who is trained in this area and can testify in court. This is likely driven by the high frequency of digital evidence gathered in traditional forms of crime rather than investigations of cybercrimes, as the rates of investigation for most types of cybercrime remain rather low. The most investigated forms of cybercrime are online fraud and scams, online harassment, and child sexual abuse material (CSAM). This reflects findings in previous research showing that local agencies in particular are more likely to investigate CSAM and interpersonal offenses compared to hacking or malware. Notably, very few agencies report investigating instances of AI-generated nonconsensual pornography, which has become of particular concern as AI models grow more sophisticated.

The agencies included in our sample indicate a high level of need and severe challenges when it comes to investigating cybercrimes and processing digital evidence. A majority of responding agencies indicated that every issue measured in the survey poses either a moderate or serious challenge to their ability to investigate. Thus, although agencies report having at least one

employee trained and assigned to investigate cyber-related crimes, there are a multitude of structural issues that make this process more difficult. This problem spans issues related to budget, available equipment, time and resources, and training for personnel. Looking at training more specifically, most agencies report a moderate or high need for training in every area. While a majority of agencies report that their investigators receive cybercrime-related in-service training, far fewer report the same for officers who are typically first responders and may be involved in initial digital evidence collection. Altogether these findings indicate that while agencies have improved investigative capabilities for basic digital evidence, the pace of this improvement lags far behind the advancement of technology and cybercrime.

Agencies report very little collaboration with third-party businesses, which has been noted in prior research as a significant challenge (Moloney et al., 2022). Proprietary hardware and software dominate the technology market, and specific skillsets are often required to properly investigate. Receiving training on more general topics is already challenging for agencies and this is exacerbated by the need for software-specific investigation. In terms of reporting cybercrime instances, only 29% of agencies report that they have criteria for classifying cybercrime or cyber-enabled crime in reports. Data on cybercrime rates are riddled with conflicting definitions and criteria, and this appears to be true at the lowest levels of reporting. The lack of guiding criteria paired with low reporting rates for cybercrime means that the cybercrime problem in the United States continues to go unmeasured at the population level.

Overall, while the data show that there has been some improvement in cybercrime response capabilities, most limitations faced by law enforcement agencies are the same as those found in research conducted several years ago. However, the expansion of agency capabilities and desire for training points to avenues for improvement.

## References


Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: an international journal of police strategies & management*, *35*(1), 165-181.

Goodison, S. E., Woods, D., Barnum, J. D., Kermer, A. R., & Jackson, A (2019). Identifying law enforcement needs for conducting criminal investigations involving evidence on the Dark Web. RAND, October 29, 2019. https://www.rand.org/pubs/research_reports/RR2704.html

Holt, T. J., Bossler, A., & Fitzgerald, S. (2010). Examining State And Local Law Enforcement Perceptions of Computer Crime. In T. J. Holt (Ed.), *Crime On-line: Correlates, Causes, and Context* (pp. 221-246). Raleigh, NC: Carolina Academic Press.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). Policing Cybercrime and Cyberterror. Raleigh, NC: Carolina Academic Press.

Moloney, C. J., Unnitahn, P., & Zhang, W. (2022). Assessing law enforcement's cybercrime capacity and capability. Law Enforcement Bulletin, April 6, 2022. https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability-

Stambaugh, H., et al., (2001). *Electronic crime needs assessment for state and local law enforcement*. US Department of Justice, Office of Justice Programs, National Institute of Justice.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal justice studies*, *29*(2), 105-124.