2010 Report on
Cyber Crime Investigation

A Report of the International High Tech Crime Investigation Association

International Office:

HTCIA, Inc.
3288 Goldstone Drive
Roseville, CA 95747

(916) 408-1751
(916) 408-7543 Fax

Todd G. Shipley
International President, 2010

Carol Hutchings
Executive Director

The HTCIA International Executive Committee Officers - 2010

President	**Todd G. Shipley** Northern California Chapter
First Vice President	**Duncan Monkhouse** Ottawa Chapter
Second Vice President	**Ron Wilczynski** Northern California Chapter
Secretary	**Art Bowker** Ohio Chapter
Treasurer	**Tom Quilty** Silicon Valley Chapter

The High Technology Crime Investigation Association

The High Technology Crime Investigation Association (HTCIA) is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Table of Contents

Executive Summary

Hardly anyone disputes that “cyber” crimes, or crimes perpetrated using digital technology and infrastructure, are a rapidly growing problem. Identity theft, child exploitation and gang recruitment are examples of crimes that make news daily. But few people understand the complexity of such cases, where evidence is often found on multiple devices and victims can be scattered across the country (or in some cases, the world). Investigators who work with these complexities find it difficult to explain them; it is easy for decision-makers to budget scarce resources to crimes they do understand, like gang violence or property crimes.

Yet digital evidence can be tied to more and more conventional crimes, so helping both police administrators, corporate executives and the public understand cyber complexities is important. Towards that end, the International High Technology Crime Investigation Association (HTCIA) surveyed its 3100+ membership about a variety of issues, including their levels of experience and training, their job functions, and the problems they experience in their day-to-day work. Of those members, 429 responded to the survey, a 13.7% response rate. HTCIA is the largest organization worldwide dedicated to the advancement of training, education and information sharing information between law enforcement and corporate cybercrime investigators.

The survey's major findings included:

Increase in criminal use of digital technology

Use of digital technologies to commit crimes has risen over the last five years. So have various types of digital crime. (Most survey respondents have worked in cyber crime investigation or digital forensics for at least the last five years, and so are qualified to estimate increases in their workloads.) While problems such as cyberbullying and stalking remain the purview of law enforcement, fraud of all kinds is a shared concern across law enforcement and private organizations.

Lack of dedicated personnel

In most members' organizations, fewer than five people are responsible for cyber crime investigations. Very often, they are assigned other duties too, so that they end up doing “a little of everything.” Such overlap leads to investigators performing digital forensic examinations, or digital forensic examiners spending time on investigations.

The reality is, investigators should be investigating, and forensic examiners should be analyzing. These issues are reflected in the comments of those who said more dedicated personnel are needed to manage investigations separately from evidence collection and analysis, and vice versa.

Need for better training at multiple levels

Many respondents did not indicate that *more* personnel were necessarily needed, but rather believed more *training* at all levels was important. A significant majority felt their colleagues' training on cyber crimes was insufficient. In fact, respondents' demands for their own training diverged from what they wanted to see for others in their organizations. For themselves, respondents want more training on digital forensics, online investigations, and computer and network security. For their colleagues, they want to see training on online investigations, collection and imaging of digital evidence, and on-site evidence preview or triage. Comments show that respondents believe training more people to handle digital evidence will reduce their backlogs, which most said were under six months' wait time. There is also a need for better public education, including employee training, about response to cyber crimes.

Training itself does not seem to be a problem. Most respondents rated the quality of their training as fair to good, and noted that they access training from a wide variety of sources: conferences, vendors, third-party providers, blogs or podcasts, and so forth. Likewise, hardware and software tools used for cyber crime and digital forensic investigations was rated satisfactory.

Need for improvements in information sharing and collaboration

Collaboration is regular and frequent among respondents, who reported that the majority of their collaborative activities include information sharing and assistance or advice seeking. Much of this, however, happens among local, state and federal law enforcement agencies, as well as regional task forces. Collaboration with academic institutions or private companies is far less common, along with outsourcing digital forensic work or assisting a company in a criminal investigation.

Need for better reporting, strategy and policy

Although two-thirds of respondents say their organizations have all three in place, the survey was not designed to determine variations in those measures. This is a concern because no standard, such as the Federal Bureau of Investigation's Uniform Crime Reporting (UCR) mechanism, exists for cyber crime reporting. Corporations governed by regulatory requirements for information security (for example, in the financial and healthcare industries) should have measures in place as required, but very little exists in as to what the policy should look like.

Membership Profile: Location and Experience

The HTCIA is divided into 40 chapters worldwide. Membership is highest in the United States, where there are 30 region-specific chapters and one at-large chapter (for those who do not reside near another chapter); 85% of membership is based in the United States. This breakdown was reflected in the survey, in which about 86% of respondents were US-based and roughly 14% came from other countries (half of those, from Canada; most of the rest from Europe and the Asia-Pacific Rim).

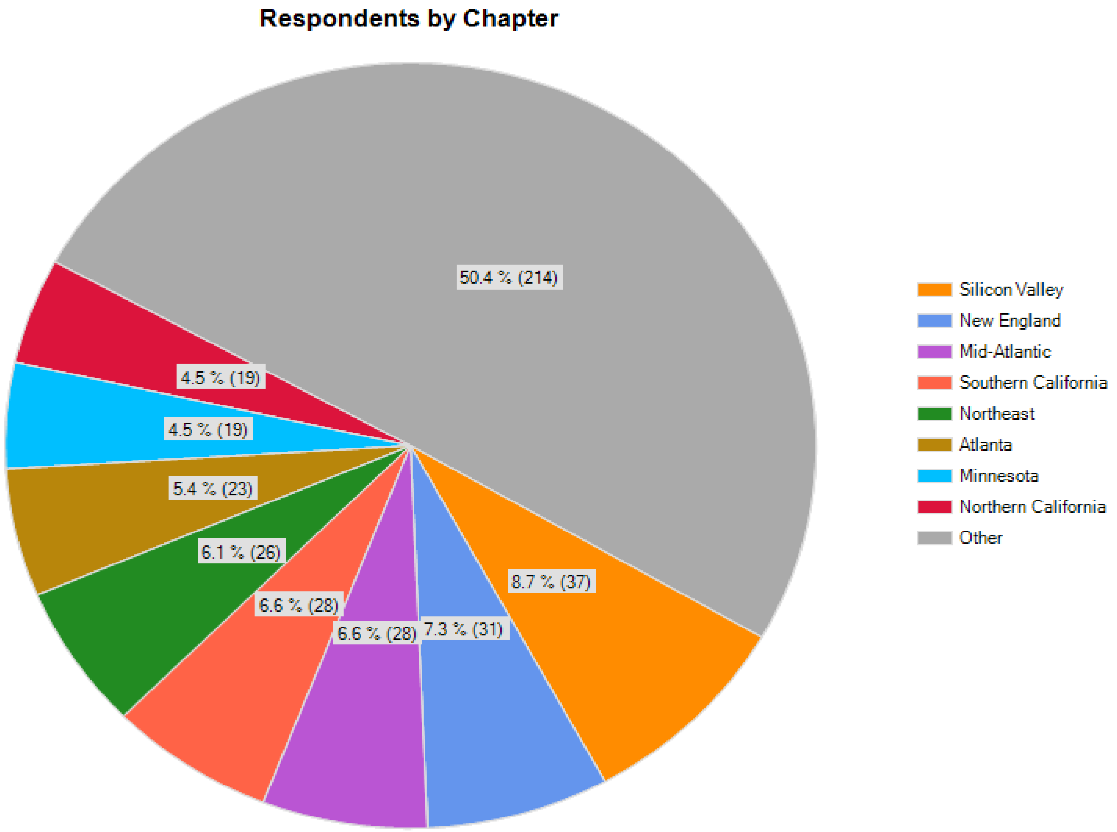

Figure 1- Respondents by Chapter

In general, HTCIA membership is about evenly divided between law enforcement/government and private/corporate employees. The organization's membership rolls reflect 55% law enforcement and 45% private, with private divided between corporate and self-employed individuals. While members were not asked specifically about their employment, their answers about their job functions and caseloads throughout the survey indicate their primary responsibilities.

Members were asked to describe their primary job functions. (Figure 2) Because job function overlap is not uncommon, especially in law enforcement agencies (as an example, a general-assignment detective may also perform digital forensic analysis part time), members were allowed to check as many as applied to them.

Nearly 71% said they were involved with digital forensics, or data recovery and analysis. One-third said they worked on incident response (commonly a corporate issue), while half identified themselves as detectives or investigators. Other job functions included corporate security or information technology, educator, and patrol officer or probation/parole/pretrial.

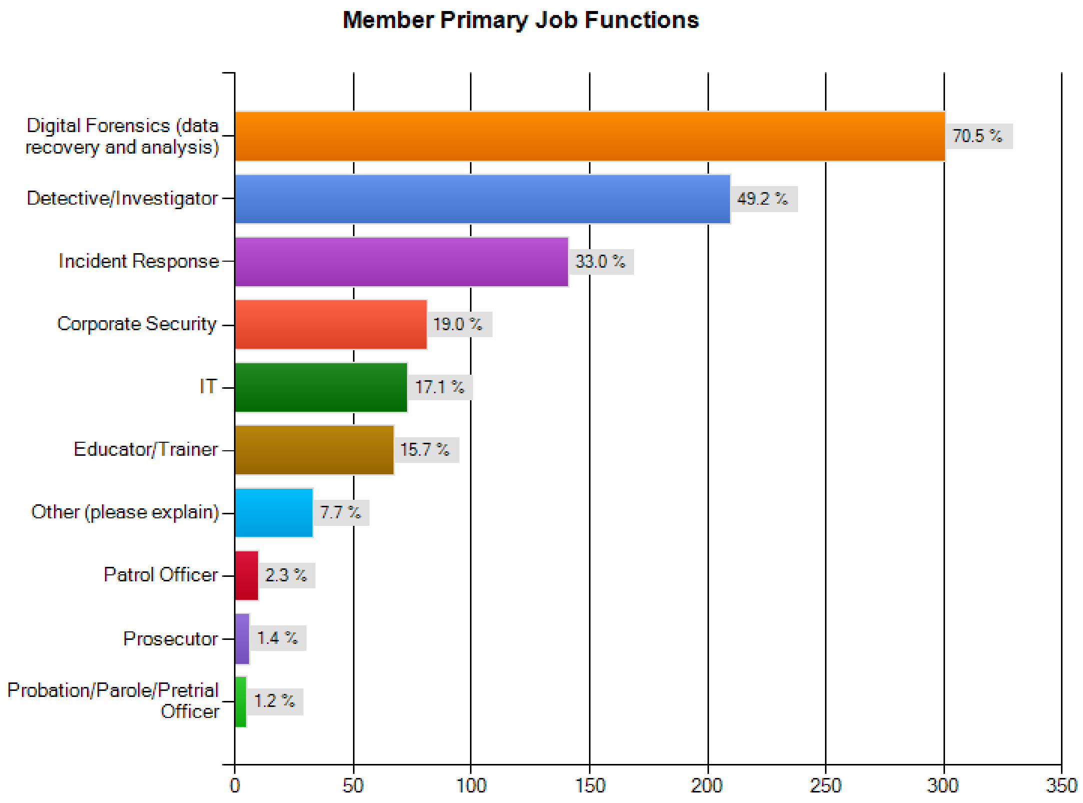

Figure 2- Members' Primary Job Functions

Members were also asked how long they had been involved in cybercrime investigations, which were defined as "investigating crimes committed with advanced technologies, of crimes committed on or through the use of the Internet." The same question was asked of digital forensics, defined as "the forensic recovery of data from computing devices, their examination and analysis, or study of same."

Because these fields are still evolving, answers were limited to 0-2 years, 3 to 5 years, or more than five years. Results indicated slightly less experience with digital forensics than with cybercrime investigations: 61% of respondents had investigated cybercrimes for five years or longer, but that dropped to 52% for digital forensic experience. Meanwhile, about 15% had investigated cybercrimes for 0-2 years, and 24% for 3-5 years, while nearly 22% and 26% had worked in digital forensics for the same periods of time, respectively.

Members' primary roles tend to encompass a wide range of activities associated with digital forensics and cyber crimes investigations, so they were asked to identify the percentage of time they devote to each of a dozen activities: (Figure 3)

Few respondents spend most or all of their time on any of the specified jobs. Respondents instead spend about 10-20% of their time on all functions, indicating that they do a little of everything. However, there are some variances. Those involved with digital forensics, for instance, gave responses more evenly distributed across 10-50% of their time. Meanwhile, nearly three-quarters of those who said they did online undercover investigations devote only about 10% of their time to the pursuit.

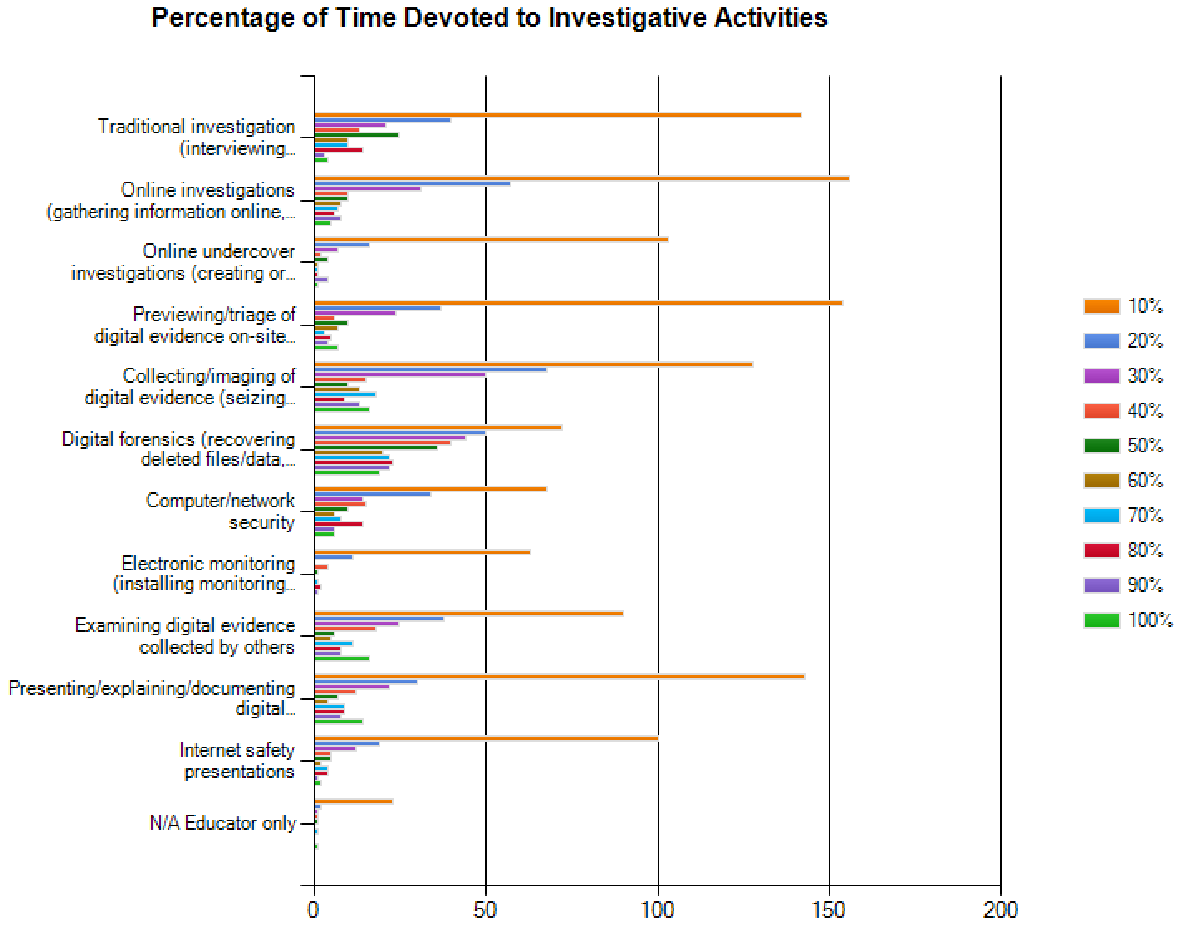

Figure 3- Percentage of Time Devoted to Investigative Activities

Criminal Activity in Member Jurisdictions

The survey asked HTCIA members to note the prevalence of computer/Internet use in their jurisdictions in the commission of an offense for each of four categories for the last five years. (Figure 4) The majority of responses indicated increases in all four categories during the past five years. Less than 1% said they had seen decreases in each of the four major categories: for research or planning to commit the offense, as a direct instrument in the offense, as a communication device between offenders and/or victims, and as a record keeping or storage device. About one-quarter noted no change in digital technology use for research or storage, while about 16% noted no change in use as a direct instrument or as a communication device.

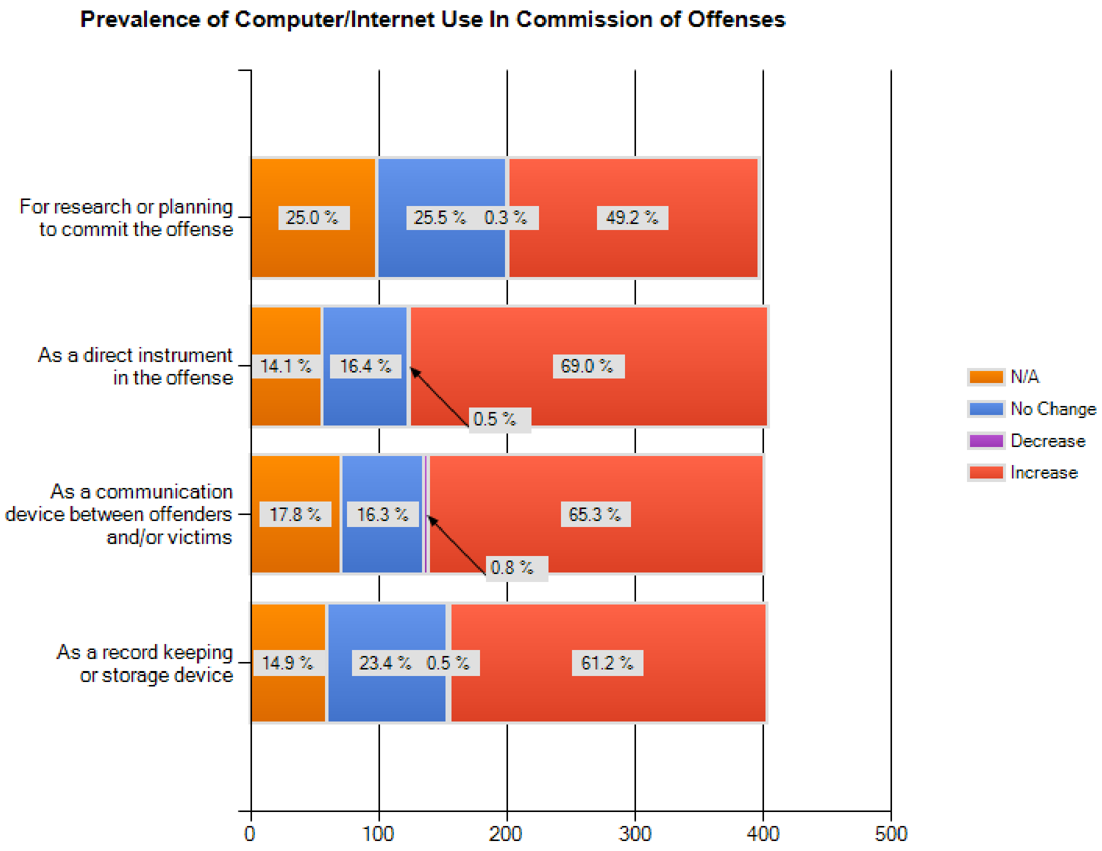

Figure 4- Prevalence of Computer/Internet Use in Commission of Offenses

Members were also asked specifically about the level of investigative activity of their agency or company on each of 14 categories for the last five years. (Figure 5) Increases were noted in all of these categories, though between one-third and one-half noted certain crimes—cyberbullying, harassment and stalking; child exploitation; malware use; gang or terrorism activity; and others were not applicable to them.[1] Meanwhile, crimes least likely to be marked "N/A" all involved fraud, including identity and intellectual property theft. These percentages are likely tied to differences between law enforcement and corporate membership.

Very few respondents indicated decreases in all these categories, while between 14-35% noted no change in the levels of activities they were seeing.

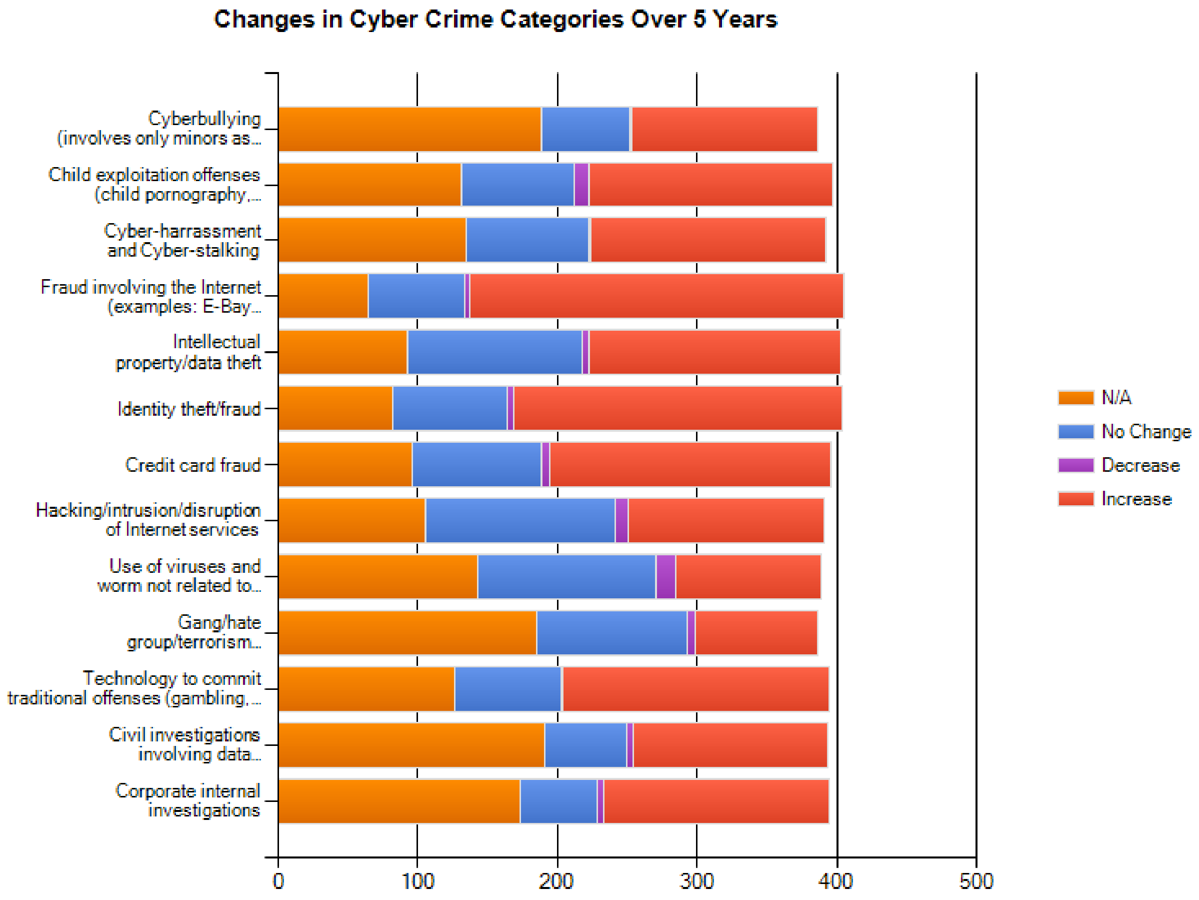

Figure 5- Changes in Cyber Crime Categories Over 5 Years

Investigators: Duties and Training

Not every investigator in an agency or company is an HTCIA member, so members were asked how many people in their organizations are responsible for cybercrime investigations (defined as investigating crimes committed with advanced technologies, incident response, forensic data

[1] Although this was not specifically asked in the survey, these investigative areas are commonly addressed by specific functional groups not general investigators; i.e; child exploitation is investigated by the Internet Crimes Against Children Task Forces, and gang and terrorism crimes are investigated by intelligence focused units.

recovery, or forensic analysis). (Figure 6)

Nearly two-thirds of respondents reported that 0-5 people were responsible for cybercrime investigations. The rest of the responses showed about even distributions among organizations where 6-10, 11-20, or 20+ people were responsible for cybercrime investigations.

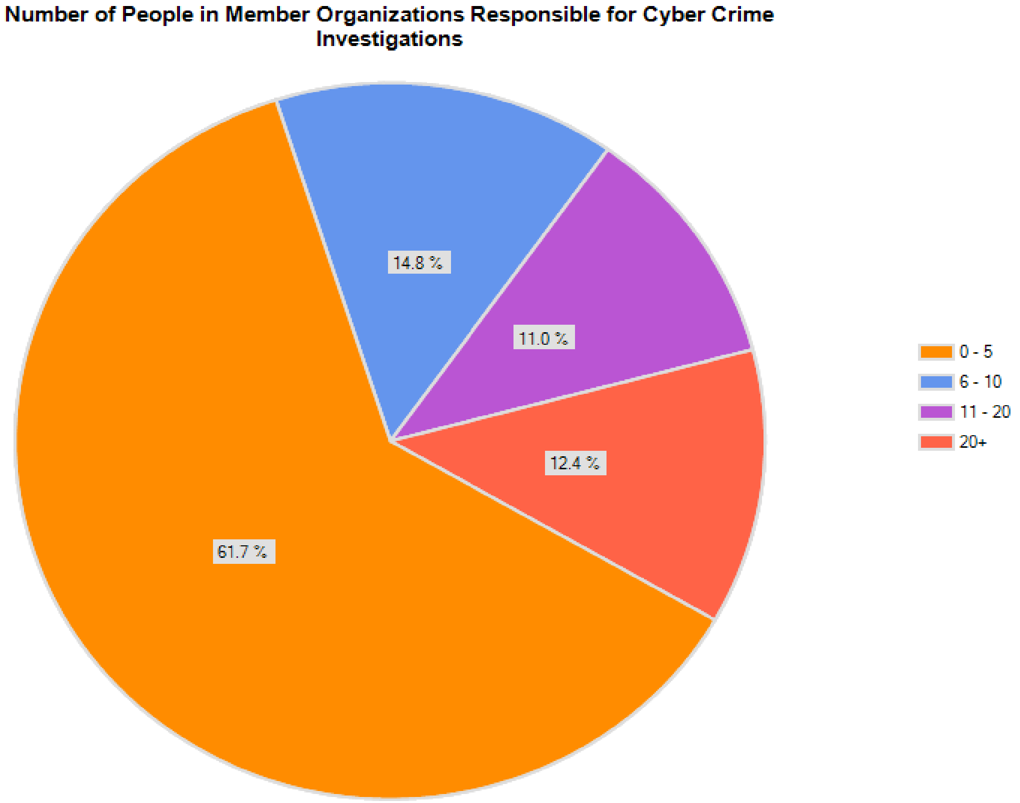

Figure 6- Number of People in Member Organizations Responsible for Cyber Crime Investigations

Because many investigators are assigned other duties, members were also asked how many of the investigators in their organizations are full time or part time. These numbers closely mirrored that of the number of people assigned to cybercrime investigations. However, 93% of respondents said 0-5 employees were part-time (i.e. assigned to other duties or caseloads).

Extensive training is necessary to keep up with the rapid changes in technology. Respondents where asked whether they thought others in their organization received sufficient training on the investigation of cybercrimes, nearly 73% responded No.

Members were also asked to rate the adequacy of their and their colleagues' training on a scale of 1 to 10. (Figure 7) One-quarter gave an “8” rating; nearly that many gave a “7” rating, and 22% gave ratings of either “5” or “6”. In other words, 75% of respondents rate their training from fair to good.

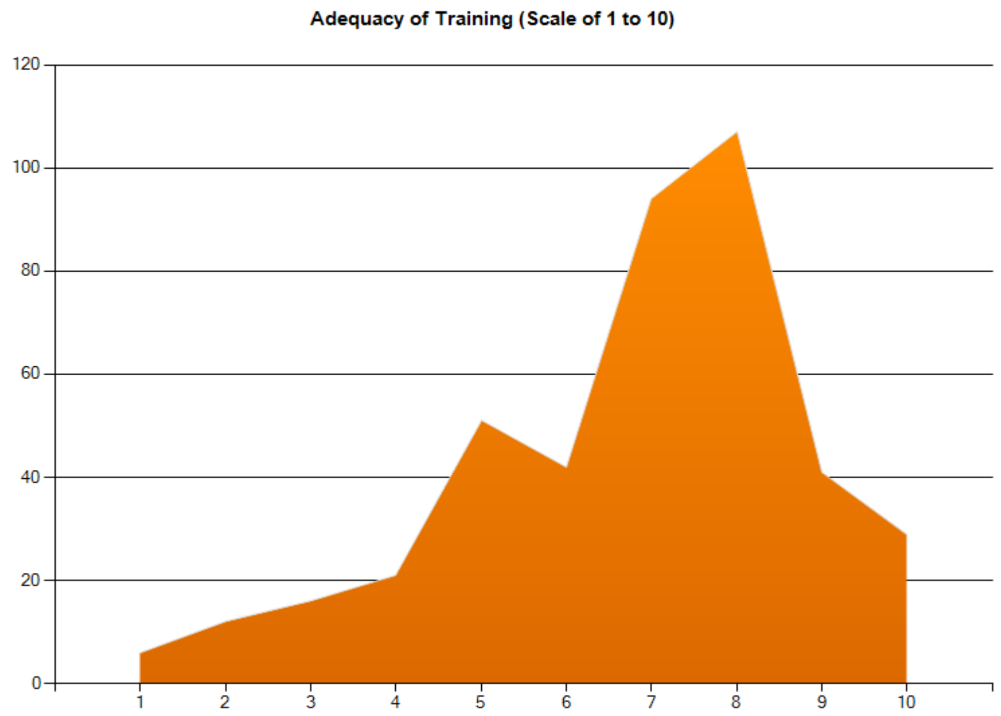

Figure 7- Adequacy of Training (Scale of 1 to 10)

The HTCIA furthermore wanted to find out whether there was a correlation between cyber crimes training and training budgets. Members were asked how much per year their organization spends on training – and how much of that is based on grant funding.

Thirty-eight percent of respondents belonged to organizations where more than $10,000 is spent per year on cyber crime training. Twenty-eight percent come from organizations that spent between $1,000 and $5,000 per year. Grant funding accounted for $0-1,000 in about 71% of respondents' organizations, indicating that most cybercrime training funding comes out of budgets rather than assistance.

The type of training investigators seek can be indicative of what types of cyber crimes they are seeing, the kind of budget they're working with, and how they view professional development. Members were asked to check all types of training and education they and their colleagues are seeking. (Figure 8)

Most actively pursue a variety of training types. Conferences are most popular; 86% of members reported seeking those. Next most popular was formal certification at around 80%, while organizational chapter meetings and free courses offered by other government agencies and contractors followed close behind. Least popular were academic degrees at 26%, while blogs and podcasts attract just 40% of respondents.

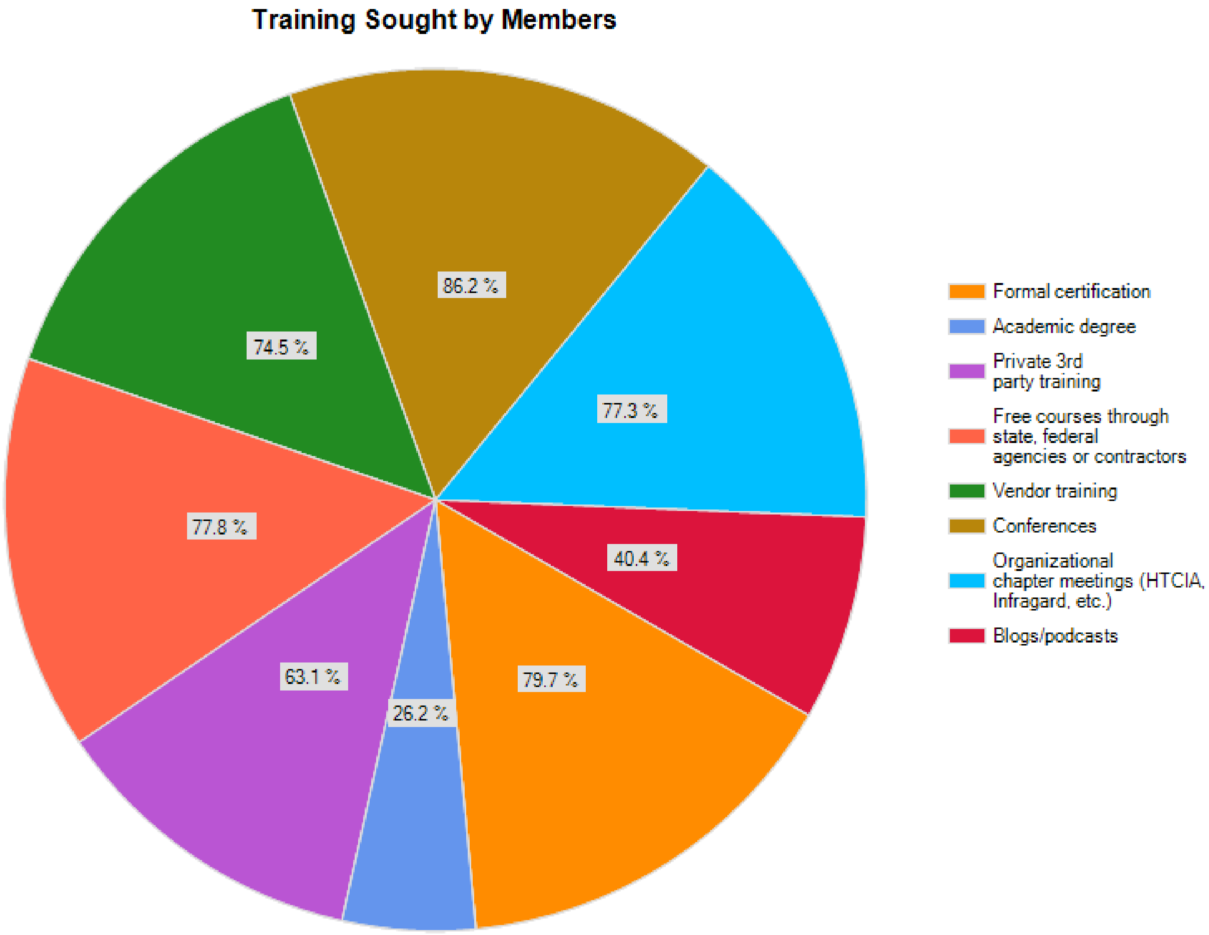

Figure 8- Training Sought by Members

Surveyed members were also asked in what specific areas of cyber crime investigation did they feel they personally, as well as others in their organization, required more training. (Figures 9, 10) Nearly two-thirds felt they needed more on the subject of digital forensics. Online investigations—not counting undercover operations—and computer/network security followed close behind. However, with regard to what they felt their colleagues needed, almost 63% wanted to see more training on online investigations. Close behind: collection and imaging of digital evidence, as well as digital forensics and evidence preview or triage.

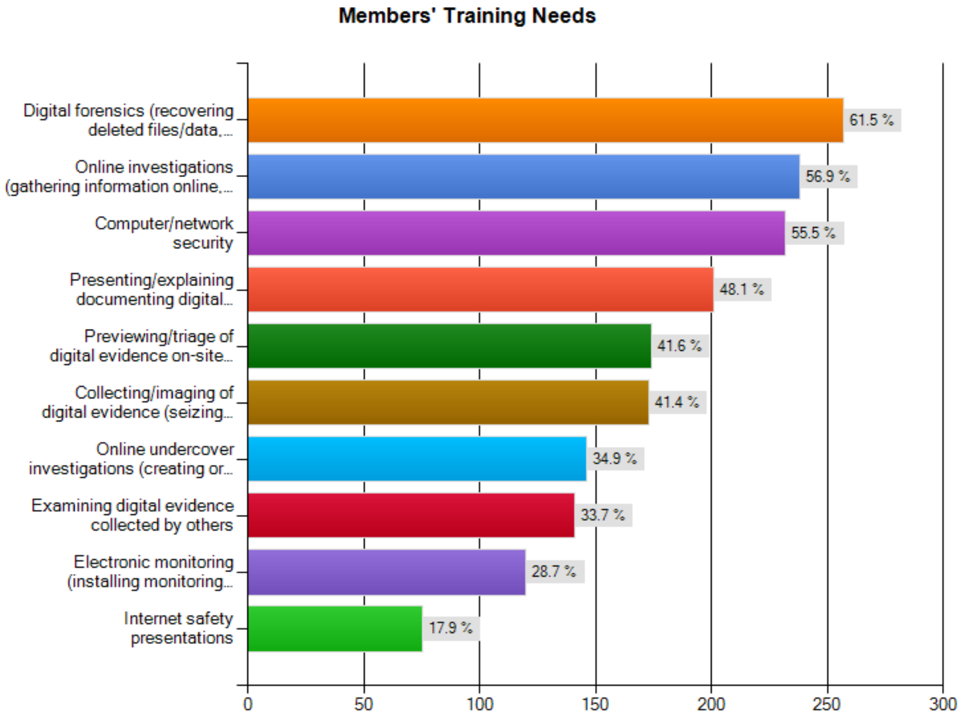

Figure 9- Members' Training Needs

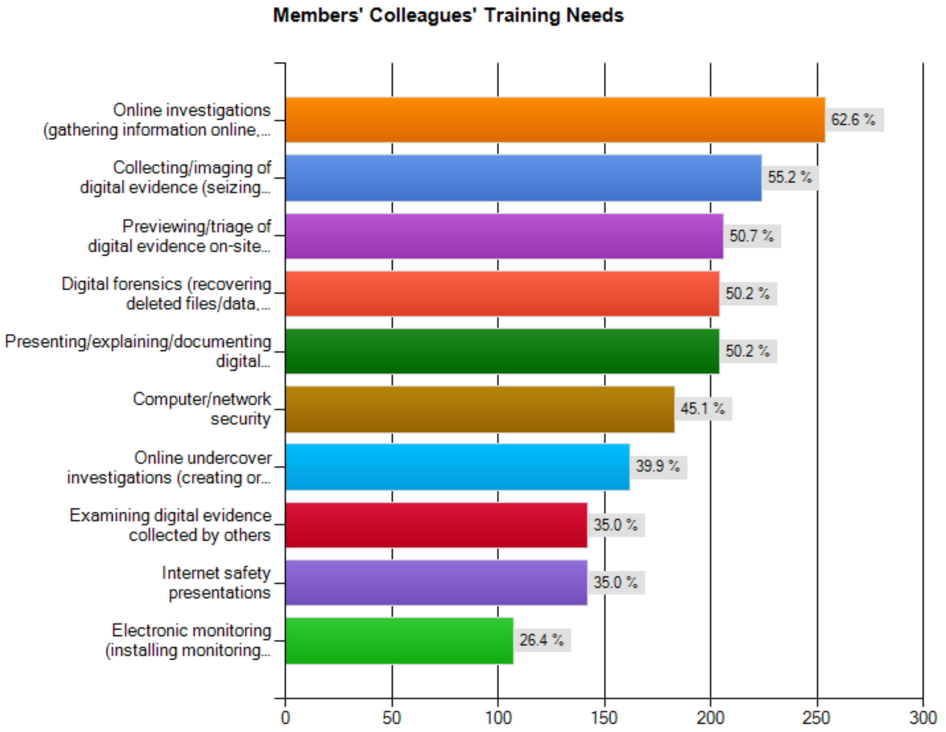

Figure 10- Members' Colleagues' Training Needs

Cooperation and Information Sharing

Members were asked how often during the investigation of cyber crimes they collaborated with another agency/company, and where those people were employed. (Figure 11) Twenty-nine percent replied that such collaboration took place weekly; another 28 percent said it took place monthly. Just 7% said they never collaborated.

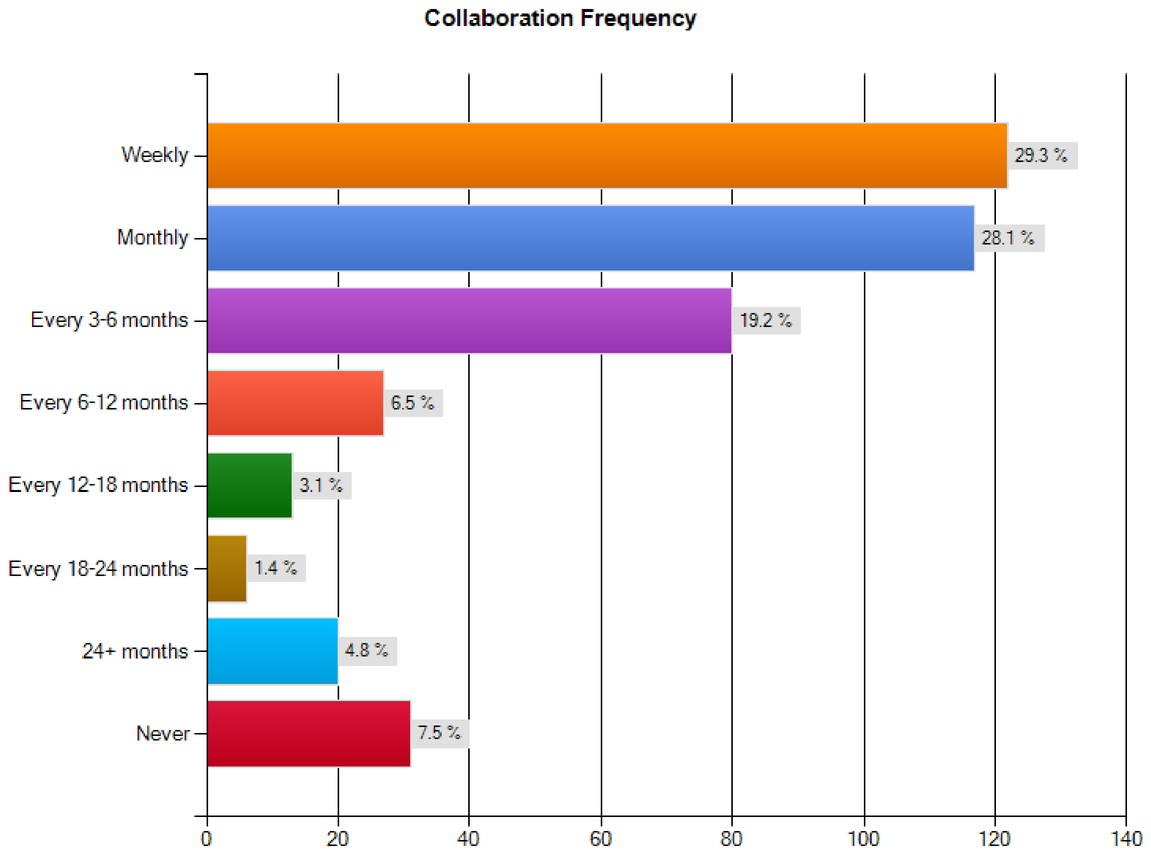

Figure 11- Collaboration Frequency

As for where the collaborators are employed, nearly two-thirds reported "other local agencies." (Figure 12) Another 57% reported U.S. government agencies. State agencies, regional task forces, and private corporations accounted for many other employers; less frequently, members reported working with people employed in academia, county agencies, or "other" government agencies.

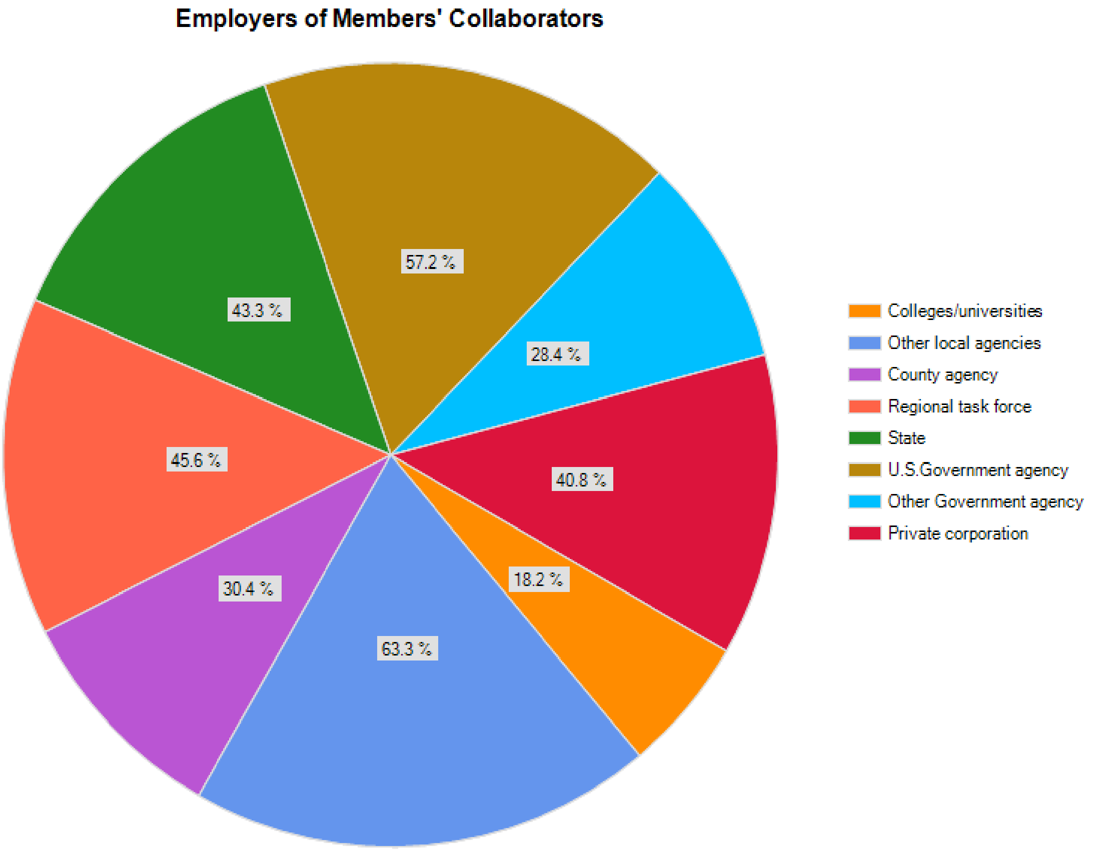

Figure 12- Employers of Members' Collaborators

Asked in what capacity the collaboration took place, members overwhelmingly reported seeking advice or assistance, along with information-sharing on tools and techniques. (Figure 13) Just 21% outsourced their digital forensic work, and investigating crimes against a company accounted for 40% of responses. Asked to define "other" types of collaboration, 36 members listed joint investigations; assistance with evidence collection, interpretation and presentation; and equipment sharing, among other roles.

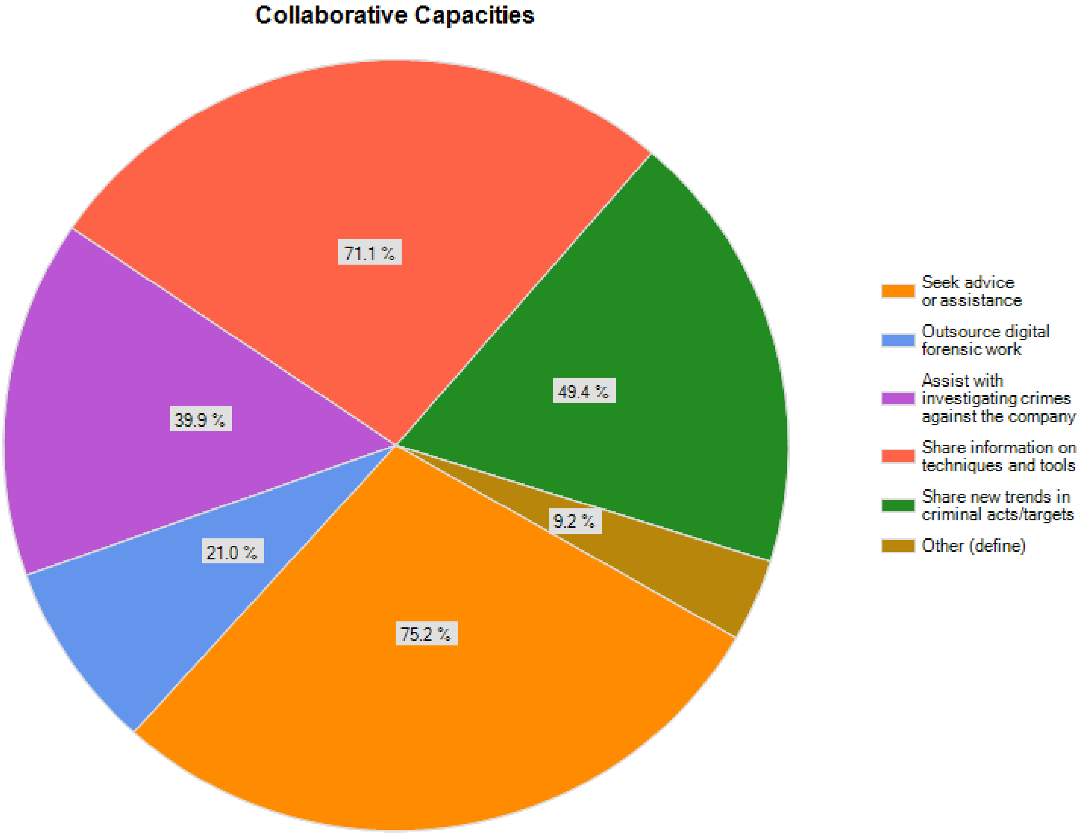

Figure 13- Collaborative Capacities

Preparedness for Dealing with Cyber Crimes

Members were asked to rate, on a scale of 1-10, the adequacy of their cyber crime investigation and digital forensic equipment (both hardware and software). (Figures 14, 15) As with training, ratings ranged from fair ("5") to good ("9"), although digital forensic equipment was rated higher than cyber crime investigation equipment.

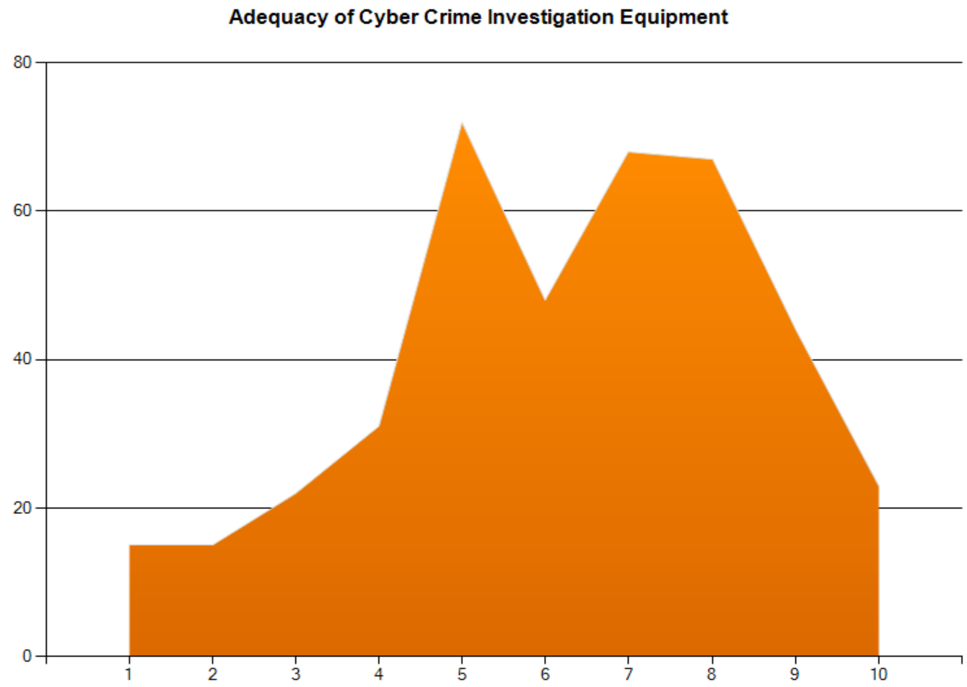

Figure 14- Adequacy of Cyber Crime Investigation Equipment

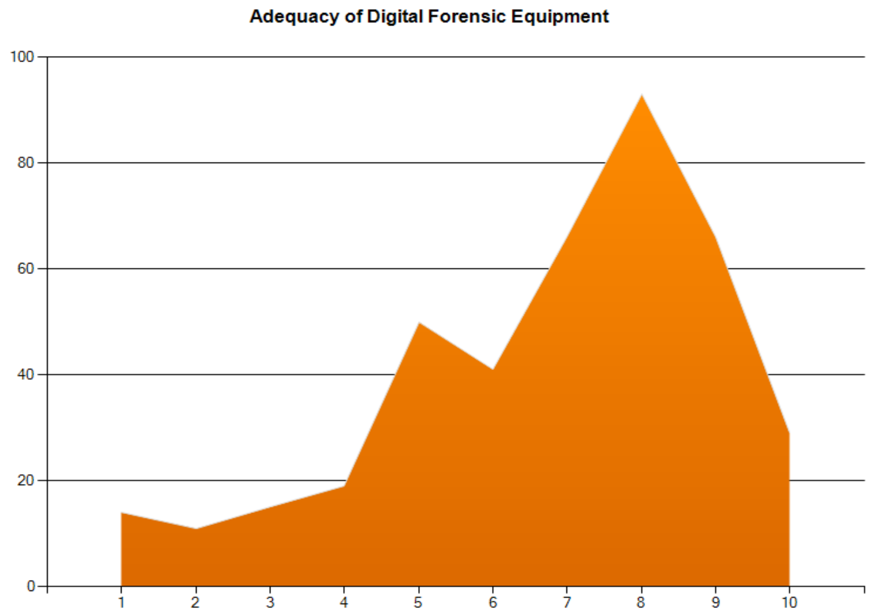

Figure 15- Adequacy of Digital Forensic Equipment

Also as with training, the adequacy of equipment is often related to budget, so members were asked how much per year their organization spends on equipment (including new purchases, annual licenses, etc.). Twenty-eight percent of the respondents noted that their organizations spent more than $20,000 per year; one-quarter said theirs spent between $1,000 and $5,000.

Backlogs in both digital and general forensics laboratories have made news headlines in recent years, so members were asked how backlogged their cyber crime investigation and digital forensic caseloads were. The vast majority reported backlogs of less than six months, though digital forensic backlogs of 6 to 12 months were reported by almost 18% of respondents, compared with 11% who reported cybercrime investigation backlogs of the same time period.

Reporting, Strategy and Policy on Cyber Crimes

The FBI's Uniform Crime Reporting system does not require law enforcement agencies to track cyber crimes, so whether an agency does this depends largely on its understanding of the significance of cyber crimes in its community. In the corporate world, meanwhile, companies in regulated industries such as healthcare are required to keep comprehensive security plans and make reports on breaches, but again, even this depends on its schooling (and sometimes even its concern with liability).

HTCIA members were asked whether their agency or company took reports on cyber crimes, as well as whether their agency or company had a strategy and/or a policy for dealing with cyber crimes. Two-thirds said their organizations do take reports; about the same number reported that their organizations had a strategy for dealing with cyber crimes, and that their organizations had also set policies.

Looking Ahead

Finally, members were asked to describe what they felt would be the five top challenges facing cybercrime investigators in the next 12 months. About half of survey respondents answered this question, which was not limited to choices, but rather, allowed members to come up with subjective answers based on their own experiences.

Responses followed similar patterns. Almost all respondents noted problems with resources. The need for better, more affordable training came up most frequently, and budget was also frequently mentioned. Less often, respondents mentioned staffing—although they did bring up the need for more dedicated cyber crimes and digital forensics investigators, along with better training for “front line” personnel on capabilities like field triage.

With regard to the actual workload investigators are dealing with, many discussed new, evolving technologies that impact caseloads and time commitments. These include data storage on the “cloud,” within mobile devices, and on larger-capacity hard drives; social networking and other forms of online investigation; and not just multijurisdictional, but also multinational investigations.

Less frequently mentioned were corporate compliance, encryption, advanced persistent threats and their relationship to cyber crimes, and the need for better proactivity: proactive investigations and public education for civilians on how to protect themselves from threats.

Conclusions

Survey respondents' answers indicate that current ways of dealing with cyber crimes are primarily reactive. That is to say, in spite of the ability to be proactive—especially with regard to catching child predators or malicious hackers—investigators are still in the position of responding to problems rather than seeking them out.

The members' responses clearly show the need for better support in the following four areas:

Public education

Public education takes up some of respondents' time, indicating that it is at least on their radar as an important activity. However, they lack time and resources to do more of it. The task often falls to detectives or prosecutors, or in the private sector, information technology professionals—who may or may not be skilled educators.

Dedicated trainers may instead benefit everyone, breaking down complex topics so that community members and employees can easily understand prevention, while organizational decision-makers can understand resource allocation needs. This approach could be likened to having state fire marshals who perform inspections and public education, freeing firefighters to focus more on their primary roles.

Organizational training

Employees of both law enforcement and corporate organizations must be better trained to handle digital evidence. Field triage, evidence previews and even rudimentary evidence collection can free investigators and forensic examiners to focus on investigative and analysis activities. The focus of the training should not just be on digital forensics. Digital evidence collection across the board comes from basic patrol activity to crime scenes, from the Internet to network intrusions. Additional organizational training should include multiple levels of education for all personnel within the organization involved in the investigation or collection of digital evidence.

Collaboration across jurisdictions

The law enforcement community is tightly knit, so resource sharing may not be troublesome for them. However, companies may need more help. Many hesitate to report crimes because they fear bad press, or in regulated industries, the possibility of being fined for failing to meet requirements.

On the flip side, too much law enforcement-corporate cooperation may concern government watchdog groups, who want to be sure that corporate interests do not have too much sway over public safety.

Collaboration is the basic tenet from which HTCIA was formed. Better collaboration and communication is a continuing challenge for any organization. This is especially true for an organization that includes a diverse mix of government and non-government members. The need, however, exists – especially in the field of digital evidence collection and examination for closer cooperation.

Reporting, strategy and policy frameworks

The fact that between 30-40% of respondents' organizations do not have reporting, strategy or policy measures in place should be cause for concern. Law enforcement needs to quantify the amount of cyber crime occurring within their jurisdictions to better grasp the magnitude of the problem. Corporations need better support on how to meet information security requirements as dictated by regulatory agencies. Both need a better understanding that virtually no investigation, either civil or criminal, comes without digital evidence in some form. Clear reporting of crimes, and subsequent investigations, provide a basis for understanding the cyber crime problem. The development of a strategic approach to dealing with the issue will allow investigators to collaborate better on investigations over the long term. Additionally, the development of policy will help to guide investigators through the complicated process of cyber crime investigations.

Appendix – 1- Methodology

HTCIA produced this report based on a survey of its membership. HTCIA is the largest cybercrime investigation organization on the world. The organization is made up of cyber crime investigators from law enforcement and corporations dedicated to the identification and arrest of persons committing crimes on the Internet.

The survey was produced at the direction of the International Executive Committee. The content of the survey was produced with the assistance of communications consultant Christa M. Miller (http://christammiller.com). The survey itself was conducted online using a commercially available internet based survey product. The survey was announced to the membership through internal membership emails and announcement on the organizational Listserv and other membership contacts.

Responses to the survey were evaluated and outlined in this report.

Appendix – 2 – List of HTCIA Chapters

Americas At-Large
Asia/Pacific Rim at Large
Europe At-Large
Arizona
Asia Pacific Rim
Atlanta
Atlantic Canada
Austin
Bay Area
Brasilia
British Columbia
Carolinas
Central California
Central Valley
Connecticut
Delaware Valley/Philadelphia
Idaho
Kansas
Louisiana
Michigan
Mid-Atlantic
Midwest
Minnesota
MO-KAN
Nebraska
New England
Northeast
Northern California
Ohio
Ontario
Ottawa
San Diego
Silicon Valley
Southern California
Southwest
St. Louis
Texas Gulf Coast
Tri-State/Pittsburgh
Washington State
Western Canadian