2011 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

H. Duncan Monkhouse
International President, 2011

Carol Hutchings
Executive Director

The HTCIA International Executive Committee Officers - 2011

President	Duncan Monkhouse Ottawa Chapter
First Vice President	Ron Wilczynski Northern California Chapter
Second Vice President	Tom Quilty Silicon Valley Chapter
Secretary	Jimmy Garcia Southern California Chapter
Treasurer	Jose Soltero Southern California 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.

Copyright Notice

Table of Contents

Executive Summary

For the first time last year, the International High Technology Crime Investigation Association (HTCIA), the largest organization worldwide dedicated to the advancement of training, education and information sharing information between law enforcement and corporate cybercrime investigators, surveyed its 3100+ membership about the challenges and solutions of cyber crime investigation as seen through their eyes. Their experience, training, equipment, and relationships within and outside of the organizations they worked for provided the context for the 2010 Report on Cyber Crime Investigation, which enabled us to draw several conclusions:

- Criminal use of digital technology was increasing
- Member respondents saw the need for more dedicated personnel to investigate cyber crimes
- Training needed to be better for those personnel
- Information sharing and collaboration needed to be improved among both law enforcement and corporate cyber crime investigators
- Organizations' cyber crime reporting, strategies and policies needed to be improved as well

This year, our membership survey saw many of the same conclusions – with a few twists. A similar cohort to last year (445 respondents, for a 14% response rate) showed:

Increase in criminal use of digital technology

For the second year in a row, our members indicated that they have seen the use of digital technologies to commit crimes, both cyber and traditional, rise over the last five years. 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, especially as it continues to rise.

Need for improvement in information sharing

At a time when many law enforcement and corporate organizations worldwide are limited in the resources and personnel they have to prevent and mitigate cyber crime, “smarter” investigation through collaboration – information and resource sharing – has become all the more important.

However, lack of resources can make it harder for investigators to connect with one another. A decrease in the frequency of information sharing between this year and last year indicates that members and others in the community need better support with their efforts. In addition, collaboration with academic institutions or private companies remains less common than sharing with other government agencies.

Need for better training at multiple levels

Civilians, judges, prosecutors and even middle and upper level management can have a hard time understanding cyber crimes. Computers and the Internet add layers of abstraction to crime; it is harder to find and collect evidence from multiple devices, and victims can be scattered across the country (or in some cases, the world). Investigators may find it difficult to explain these complexities, but without understanding, decision-makers find it easier to budget scarce resources to (or in judges' case, set legal precedent for) crimes they do understand, can see, and have a measurable impact on, like narcotics or property crimes.

Many respondents indicated a need for better training for others in their organization, especially for managers, and better training in how to explain digital evidence. A need for better computer security training received more emphasis this year than last, possibly because of so much media attention placed on data breaches, malware and similar incidents. Overall, however, member respondents continue to desire more training in digital forensics and online investigations, as well as on-site preview or triage responsibilities.

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. Just as it did last year, this remains a concern because no standard, such as the Federal Bureau of Investigation's Uniform Crime Reporting (UCR) mechanism, exists for cyber crime reporting. Perhaps more importantly, law enforcement agencies and corporations may have widely divergent policies and strategies based on the extent to which the understand the problem of cyber crime.

Membership Profile: Location and Experience

The HTCIA is divided into 41 chapters worldwide. Membership is highest in the United States, where there are 31 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 close to 85% of respondents were US-based and roughly 14% came from other countries. Of those, 10% came from Canada (an increase from last year's survey); the rest of the responses came from Europe, the Asia-Pacific Rim, and Brazil.

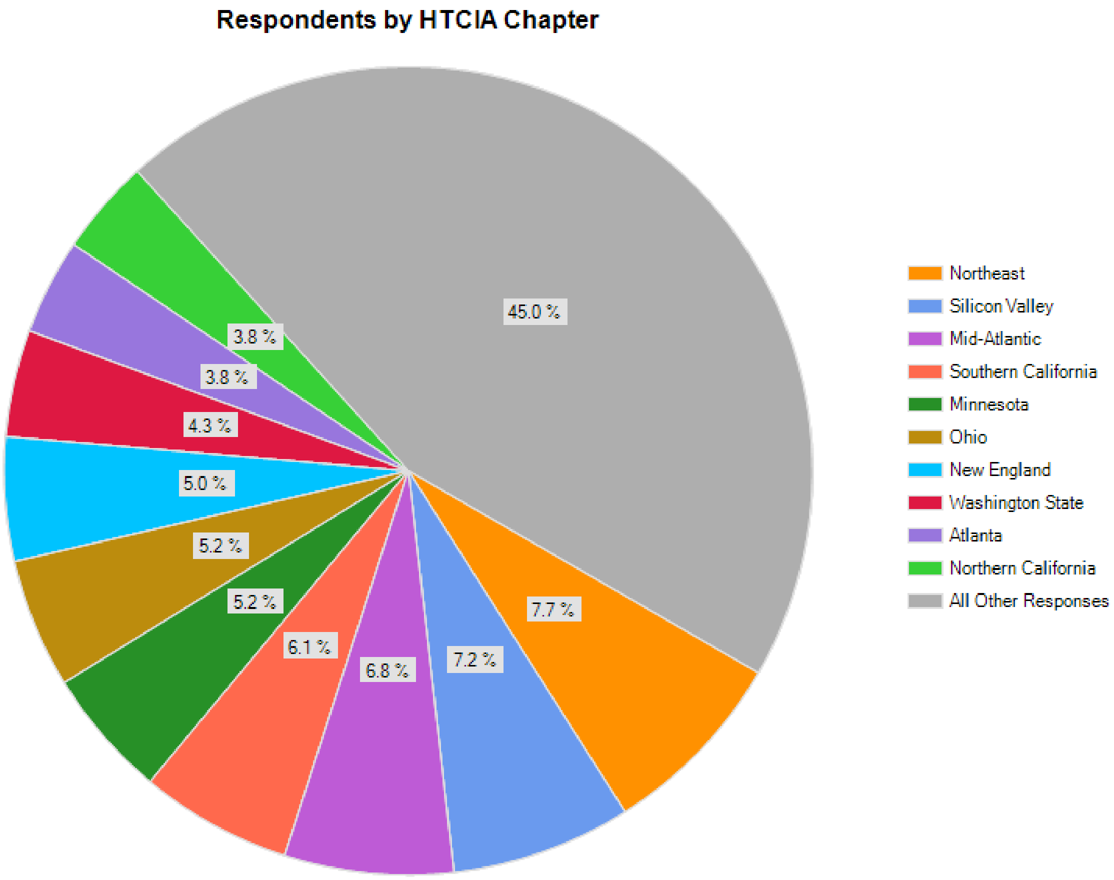

Figure 1- Respondents by Chapter

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.

Just under 70% said they were involved with digital forensics, or data recovery and analysis. This represented a decrease from last year, as did the 42% of self-identified detectives or investigators, 29% of incident responders, and 18% of corporate security. However, the 23% of respondents who said they worked in information technology (IT) and the 16% of educators and trainers represented increases in both categories since last year. The number of responding prosecutors and probation/parole/pretrial officers also increased – by about half in each case – while the percentage of patrol officers remained the same.

About 11% of respondents checked “Other”. In the open-response box that followed, they reflected roles in electronic discovery, senior or executive management, consulting, and the legal field. Vendors, counterintelligence and counterespionage, information assurance and even some physical forensic science professionals were also represented. Future surveys will likely take many of these specifics into account in order to generate more accurate responses.

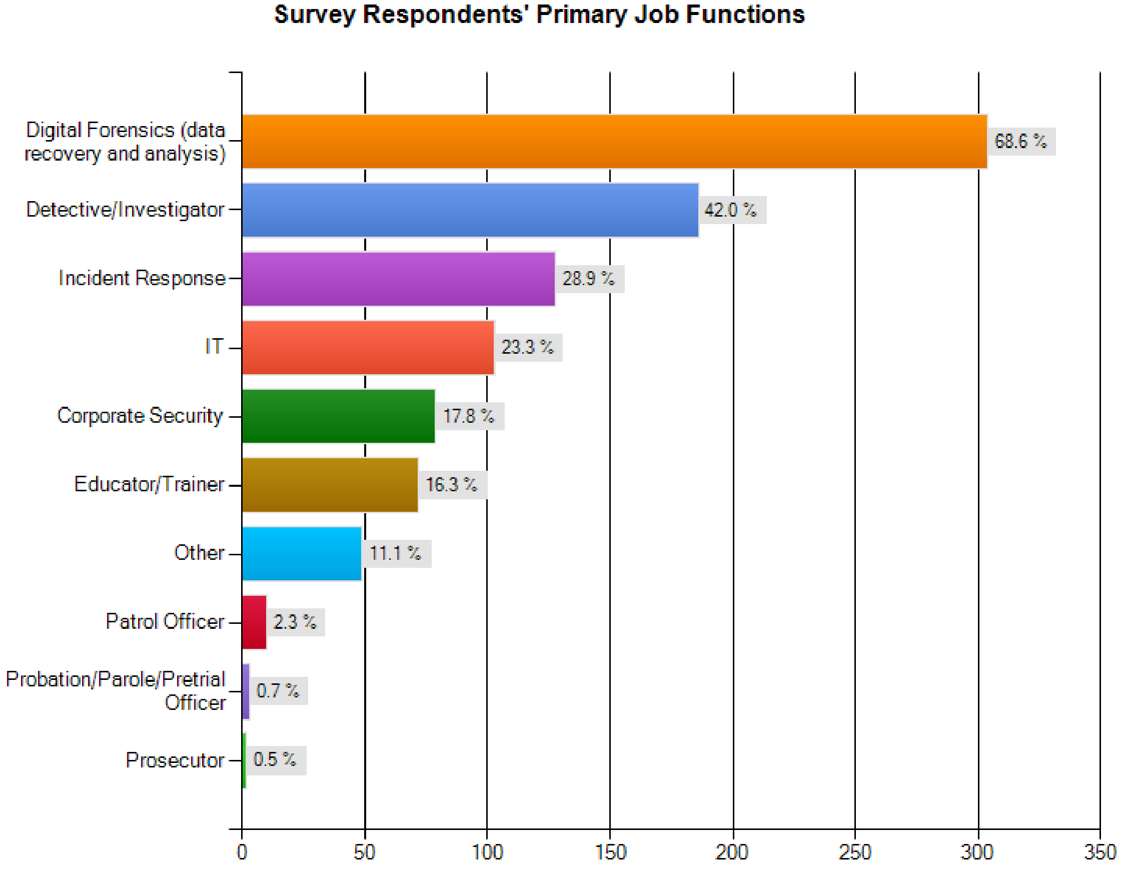

Figure 2- Respondents' Primary Job Functions

This year, as last year, we asked our member respondents how long they had been engaged with digital forensics and cyber crime investigation. In response to feedback from last year's survey, which asked for a more accurate reflection of our entire community, we added two additional fields: electronic discovery and network security.

Because these fields continue to evolve, answers were again limited to 0-2 years, 3 to 5 years, or more than five years. The majority of respondents were involved with digital forensics and cyber crime investigation rather than with e-discovery or network security. However, of all four fields, only those involved with e-discovery were not as likely to have more than five years of experience.

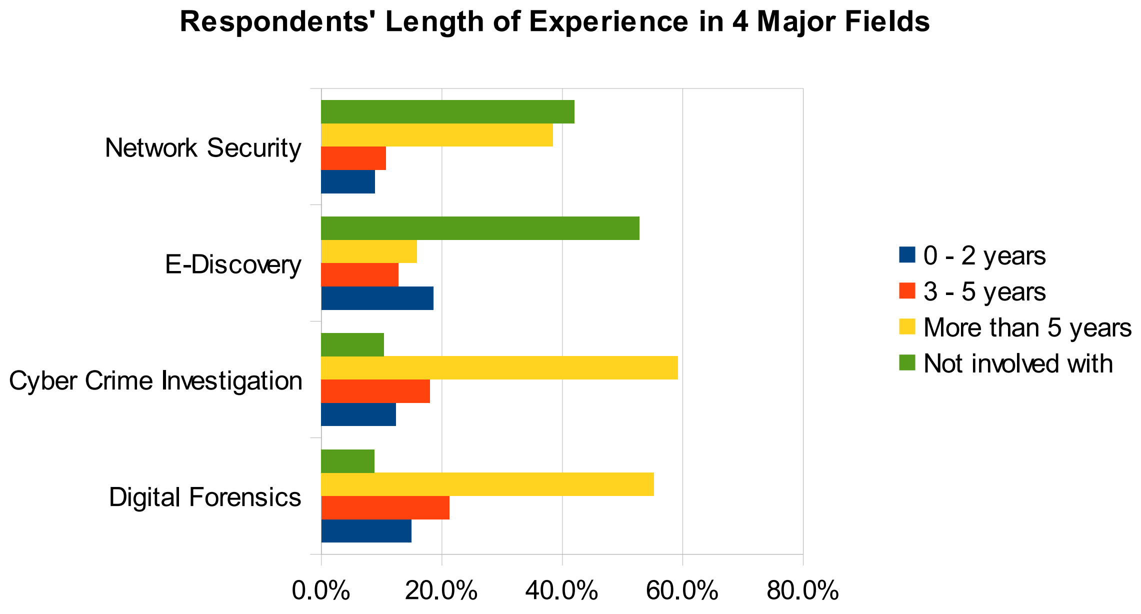

Figure 3- Respondents' Length of Experience in Major Fields

Members' primary roles tend to encompass a wide range of activities associated with digital forensics and cyber crimes investigations. Whereas last year, they were asked to identify the percentage of time they devote to each of a dozen activities, this year, they were asked to rate the importance of each function to their work. This change was made in order to get a more accurate representation of how respondents actually view their work. (Figure 4)

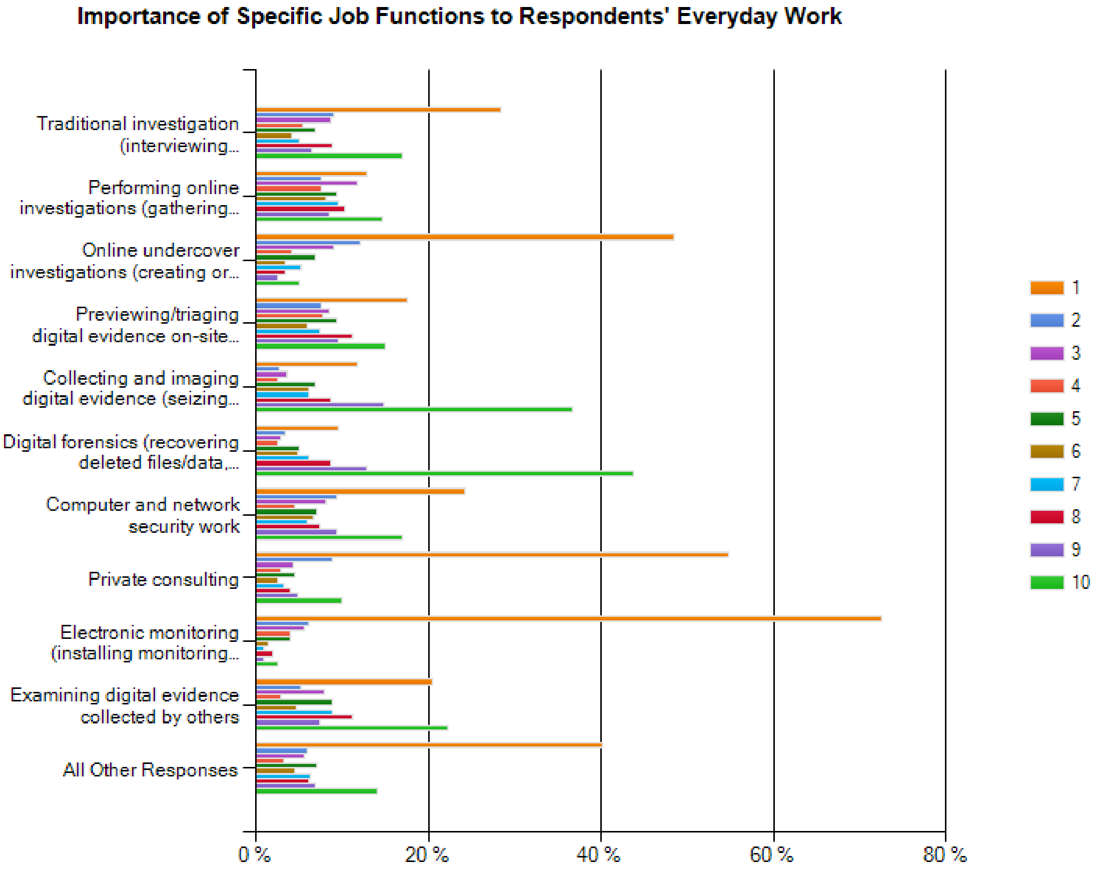

Figure 4- Percentage of Time Devoted to Investigative Activities

The job functions rated as being most important among member respondents were collecting and imaging digital evidence; digital forensics; and presenting, explaining and/or documenting digital evidence. Of those, nearly half (44%) of respondents rated digital forensics a 10. Another 37% gave the same rating to the collection and imaging of digital forensics, while 29% rated the presentation of digital evidence a 10.

By contrast, the job functions rated least important to respondents were online undercover work, private consulting, electronic monitoring, Internet safety presentations and teaching in higher education. Online undercover work received a rating of 1 from 48% of respondents, while 55% reported private consulting as least important to them. Nearly three-quarters said electronic monitoring was not important to their responsibilities. Two-thirds rated teaching in higher education a 1, while 42% gave the same rating to making Internet safety presentations.

Other job functions that received ratings of 10 also received ratings of 1 from a similar percentage of respondents. For instance, online investigation was rated 1 by 13% of respondents, but got a 10 from 15%. (This function received a fairly even distribution of ratings.) Preview or triage rated 1 on 17% of respondents' scales, but rated 10 for 15% of respondents. Computer and network security was least important to 24% of respondents, but most important to 17%. The examination of digital evidence collected by others was most important to 22% of respondents, but least important to 21%. Meanwhile, traditional investigation was least important to 28% of respondents, but most important to 17%. Nearly all the job functions in this category saw U-shaped distributions, where comparatively fewer respondents gave middling ratings.

Criminal Activity in Member Jurisdictions

The survey asked respondents 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 5) The majority of responses indicated increases in all four categories during the past five years; however, these increases were noted by lower percentages of respondents, while the percentages of "Not Applicable" responses increased across all categories.

As an example, 61% of respondents in 2010 reported increases in computers or the Internet being used for record-keeping or storage, while 15% reported that this was not applicable to their work. In 2011, however, only 55% of respondents said they had seen increases in digital record-keeping, while 23% indicated that this usage was not applicable.

Meanwhile, one percent or fewer said they had seen decreases in each of the four major categories. About one-fifth noted no change in digital technology use for storage or research, while 14-15% noted no change in use as a direct instrument or as a communication device.

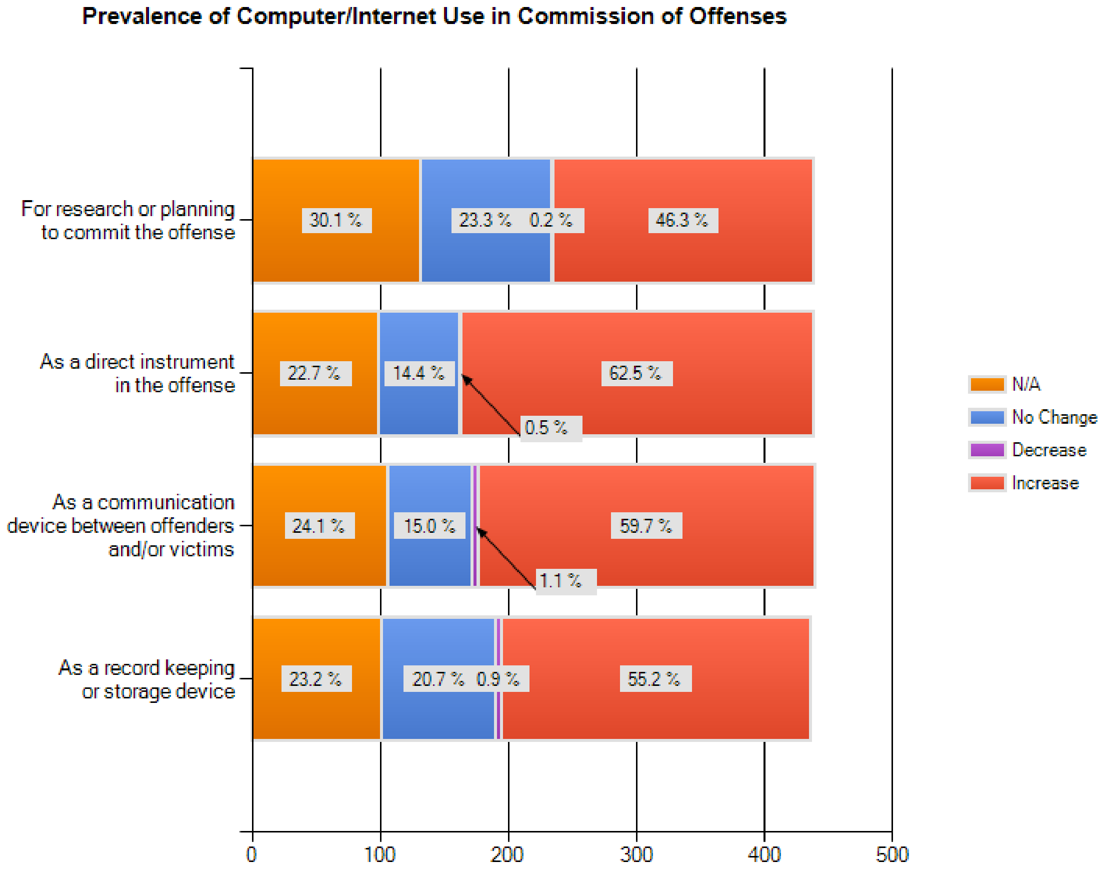

Figure 5- Prevalence of Computer/Internet Use in Commission of Offenses

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 6) As in 2010, 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.

Very few respondents indicated decreases in all these categories, while between 16-32% noted no change in the levels of activities they were seeing. And in some notable instances, there were marked differences between percentages this year versus last year.

For example, last year, 66% of respondents noted an increase in Internet-related fraud; this year, that percentage dropped to 57%, while the percentages of "no change" and "not

[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.

applicable" responses rose by five points each (17% to 22% and 16% to 20% respectively) for that category. Likewise, in 2010 48% of respondents reported an increase in the use of technology for traditional crimes, but in 2011, that percentage was just 38%. The number of "no change" responses in that category rose correspondingly.

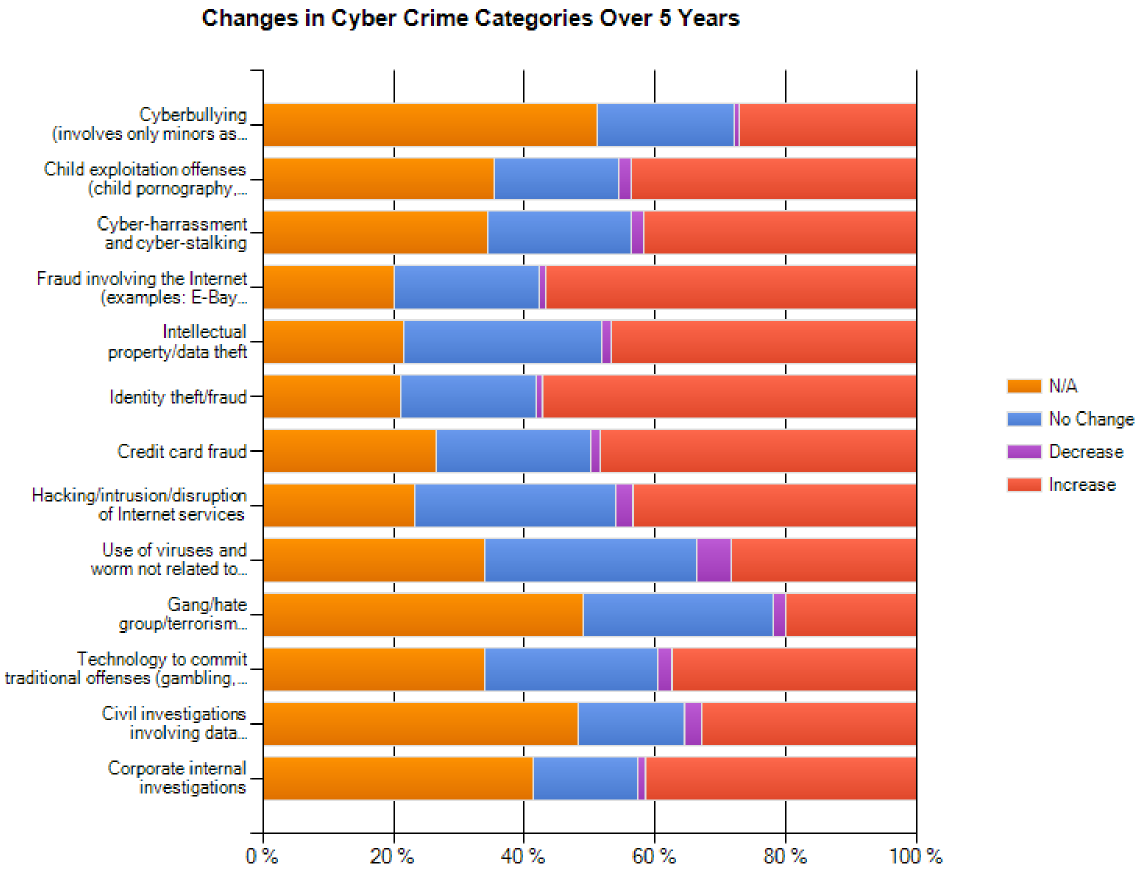

Figure 6- Changes in Cyber Crime Categories Over 5 Years

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 recovery, or forensic analysis).

As in 2010, nearly two-thirds of respondents reported that 1-5 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. Five percent of respondents indicated that no one in their organizations were responsible for cybercrime 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. Fifty-eight percent of respondents said their organizations employed between one and five full-time cyber crime investigators; 13% said they had no full-time investigators, while the remainder said there were 6-10, 11-20, or more than 20 full-time investigators. Seventy percent of respondents reported no part-time cyber crime investigators, although more than a quarter said their organization employed between one and five part-timers. Only 4% of respondents reported working with six or more part-time cyber crime investigators.

Extensive training is necessary to keep up with the rapid changes in technology. Asked whether they thought others in their organization received sufficient training on the investigation of cybercrimes, nearly 58% of respondents said No. However, this was a decrease by 15% from last year.

Members were also asked to rate the adequacy of their and their colleagues' training on a scale of 1 to 10. In an increase from last year, nearly 30% gave an “8” rating (an increase of about five percent from last year); about one-fifth gave a “7” rating, and the same number gave ratings of either “5” or “6”. In other words, nearly three-quarters of respondents rate their training from fair to good.

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.

In 2010, 38% of respondents belonged to organizations where more than $10,000 was spent per year on cyber crime training. This year, however, that percentage dropped to about 24%. About 35% said their organizations spent between $1,000 and $10,000; in 2010, 46% had reported this level of expenditures on training.

However, respondents who said their organizations spent $1,000 or less on training increased only from 15% in 2010 to 19% in 2011. Less than 5% of respondents reported their organizations spent nothing on cyber crime investigation training. Only 16% of respondents indicated that grant funding was used for any of their training expenditures, 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 7)

Most actively pursue a variety of training types. While last year, respondents most frequently sought training from conferences (at a rate of 86%), this year, that percentage decreased to 82%. Meanwhile, organizational chapter meetings rose in popularity to 83% from 77%. Next most popular was formal certification at around 80%, a percentage similar to last year's, while free courses offered by other government agencies and contractors followed at 73% (a drop from 78% last year) and vendor training was sought by 74% of respondents (a slight decrease from last year). The demand for private third-party training, however, rose slightly from last year to this year. Least popular were academic degrees at 24%, while blogs and podcasts attract 47% of respondents (up 7% from last year).

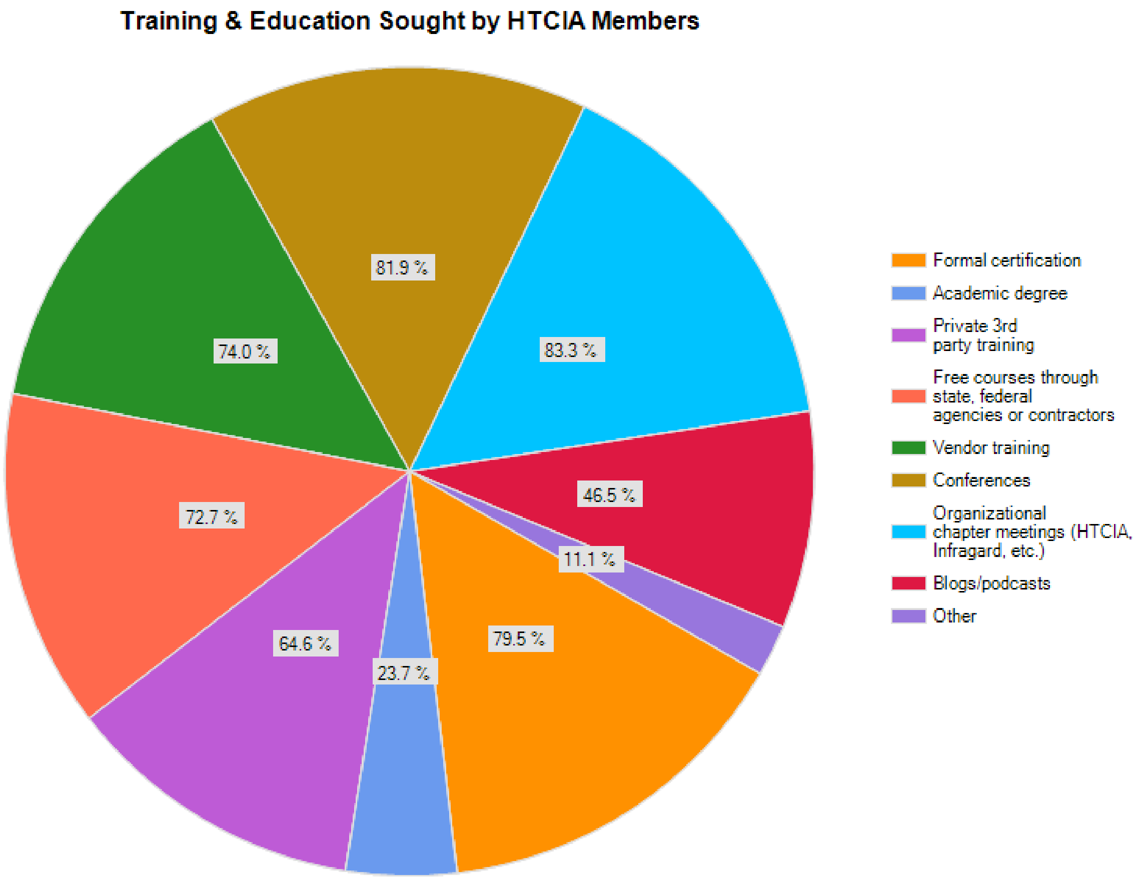

Figure 7- Training & Education Sought by Members

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 8, 9) Just over 60% felt they needed more on the subject of digital forensics. Computer/network security followed close behind at 56%, with online investigations third at 53%. The latter two represented somewhat of a reversal from 2010: then, 57% wanted more online investigations training, while 55% wanted more security-related training.

However, with regard to what they felt their colleagues needed, for the second year in a row a majority (61%, compared to 63% last year) wanted to see more training on online investigations. Close behind: collection and imaging of digital evidence, evidence preview/triage, digital forensics and computer/network security. In a second reversal, more respondents this year wanted their colleagues to have more training in computer/network security (51%) than in the presentation of digital evidence (44%). In 2010, those percentages were 45% and 50% respectively.

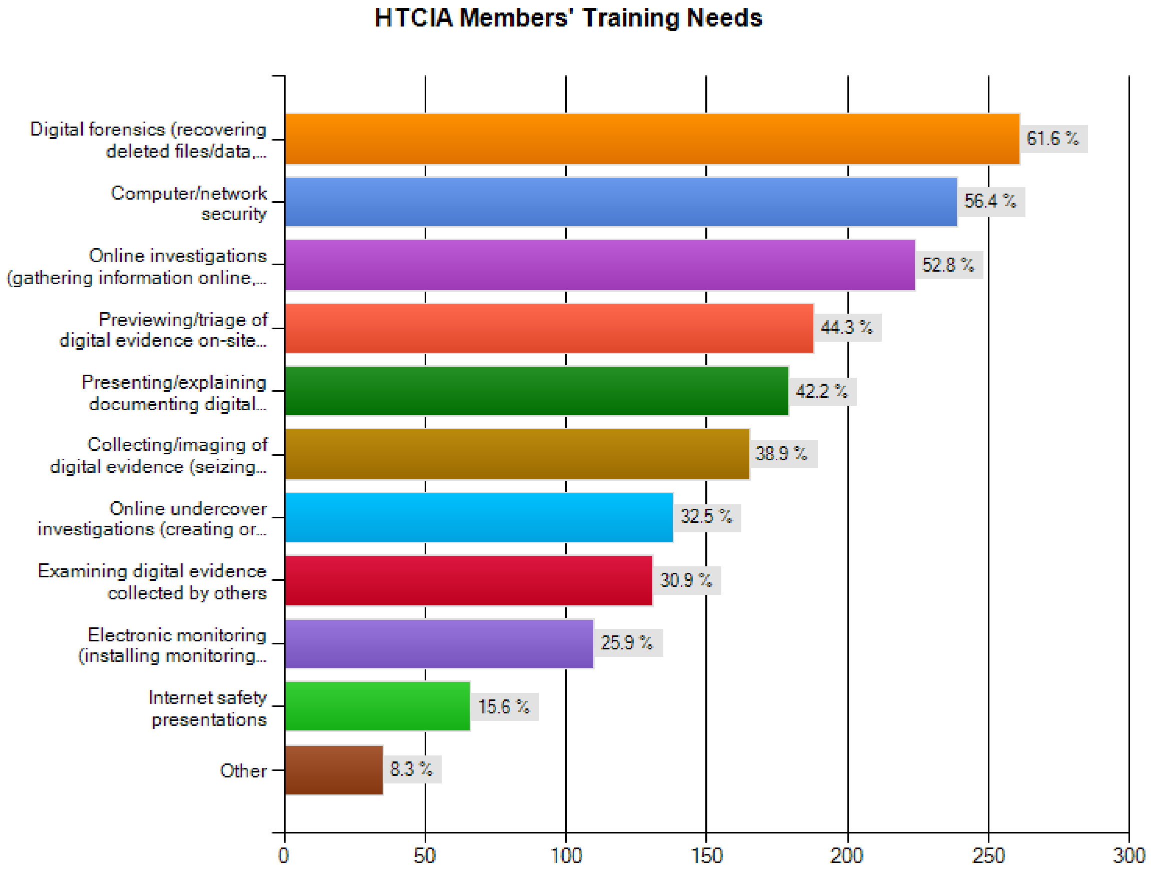

Figure 8- Members' Training Needs

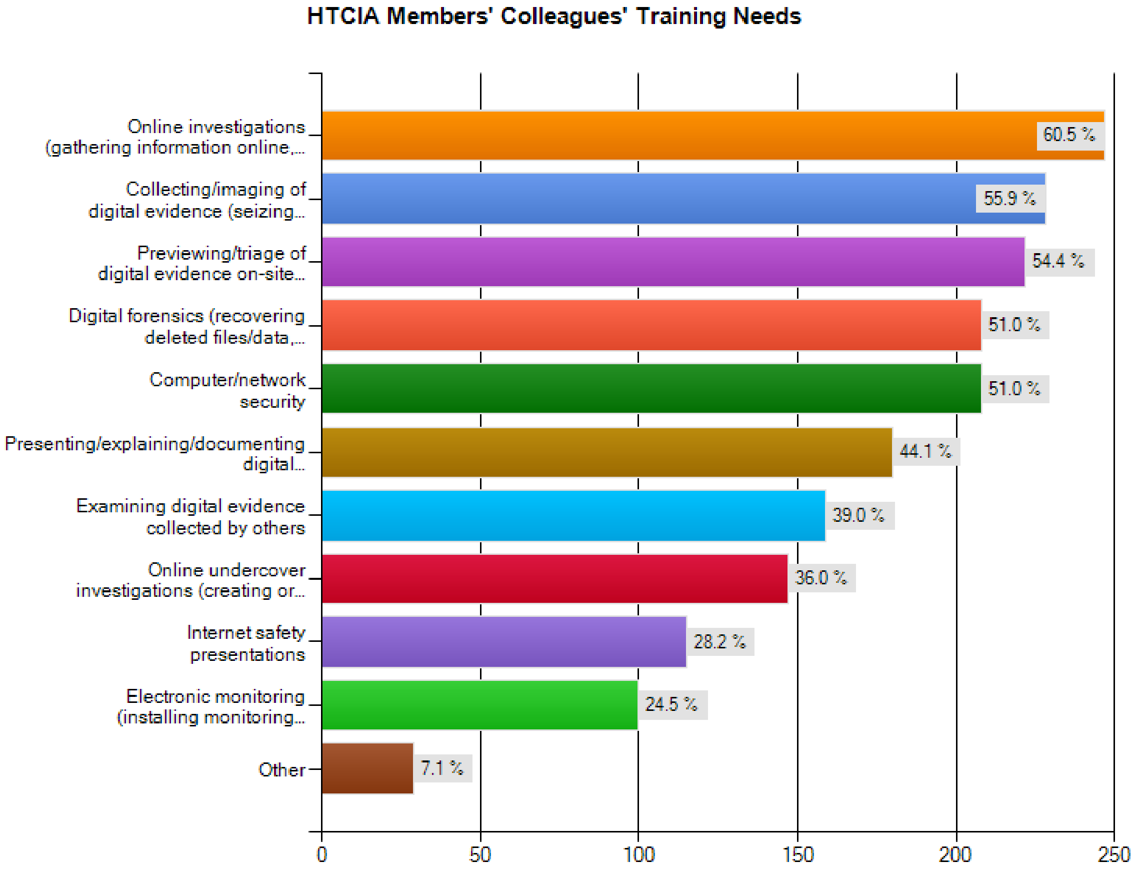

Figure 9- Members' Colleagues' Training Needs

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 10) Twenty-one percent replied that such collaboration took place weekly; another 30% said it took place monthly. Ten percent said they never collaborated.

These numbers changed since last year, when 29% of respondents reported collaborating weekly with other agencies or companies, and 28% collaborated monthly. Small increases were reported between 2010 and 2011 in the other time spans, although only 7% of respondents last year said they never collaborated.

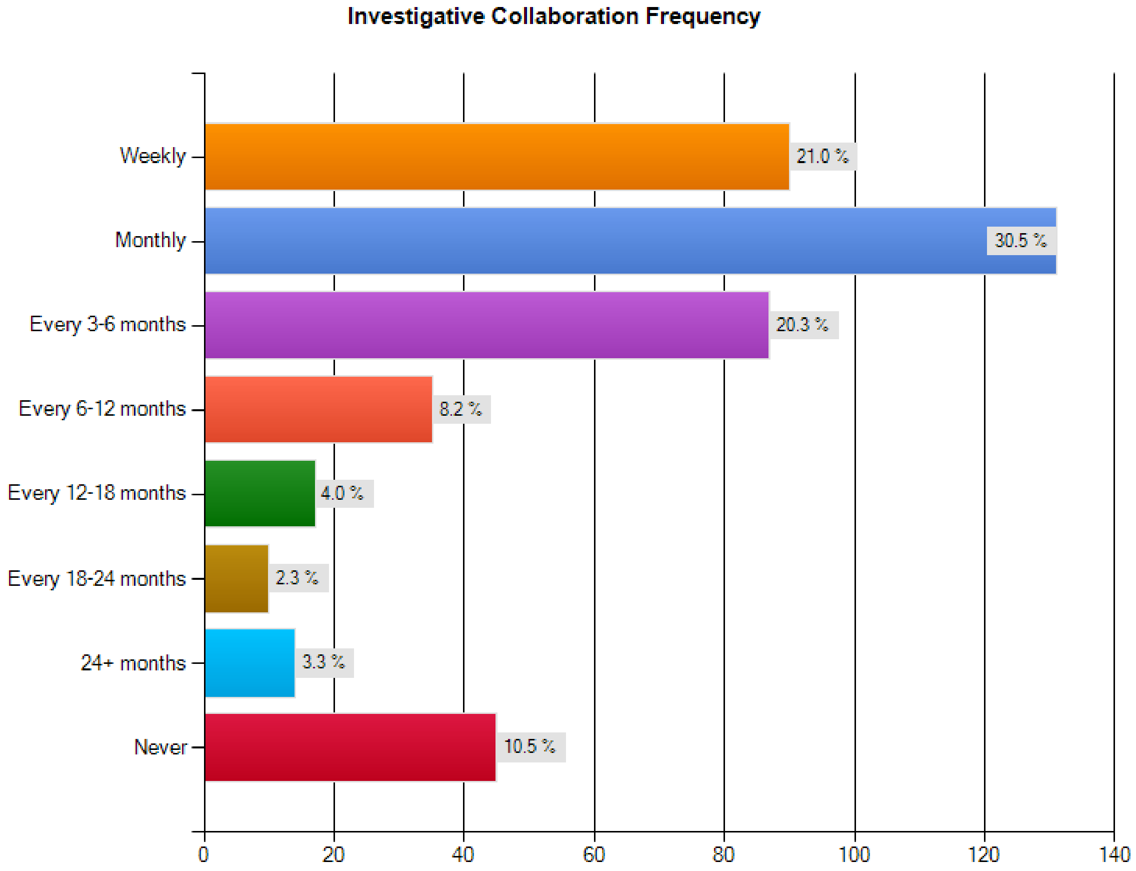

Figure 10- Collaboration Frequency

As for where the collaborators are employed, about 60% reported "other local agencies." (Figure 11) Another 50% reported U.S. government agencies; both represent decreases from last year. State and county agencies, regional task forces, and private corporations accounted for many other employers; less frequently, members reported working with people employed in academia or "other" government agencies. Between 2010 and 2011, the percentage of collaborations with all types of organizations decreased, although collaborations with colleges and universities rose slightly. Collaborations with task forces declined by about 14%, with "other" government agencies by about 10%, and with US government agencies by about 7%.

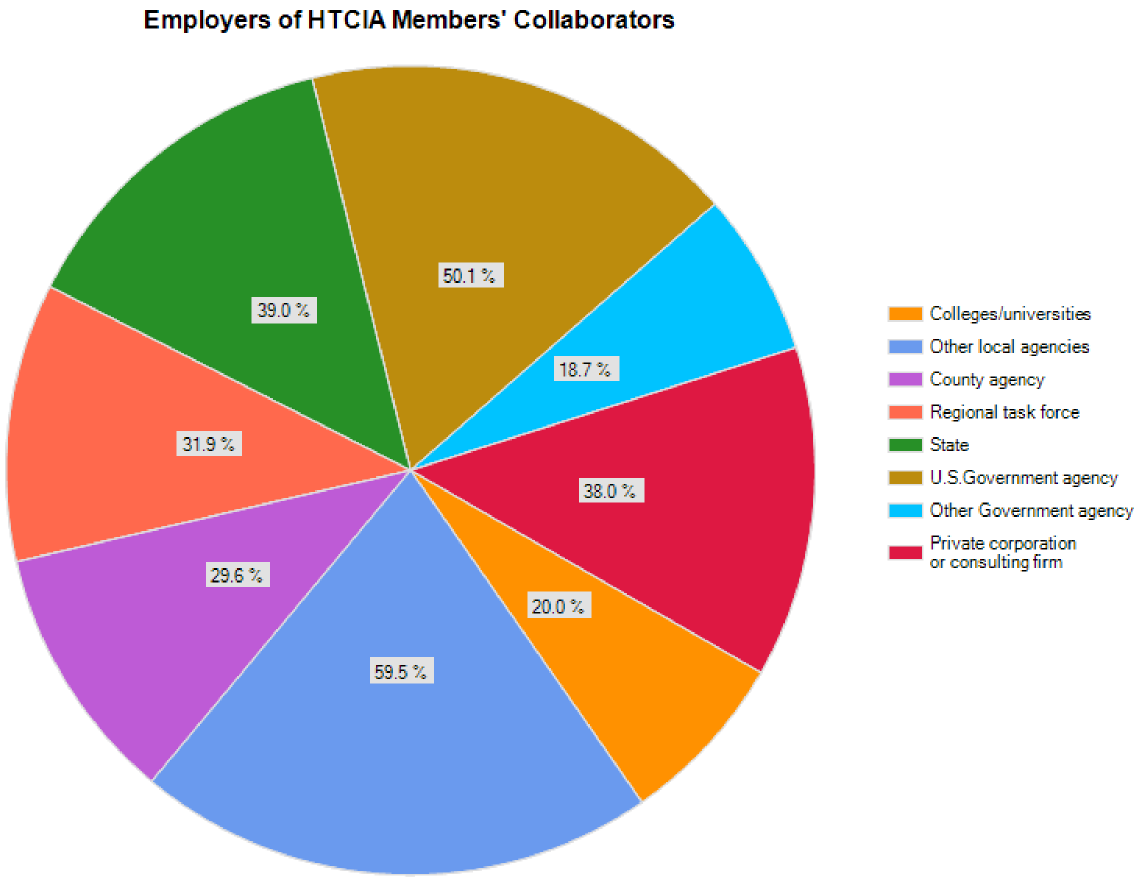

Figure 11- Employers of Members' Collaborators

Asked in what capacity the collaboration took place, members overwhelmingly reported seeking advice or digital forensic assistance, along with information-sharing on tools and techniques. (Figure 12) Half of collaborations involved joint investigations. Just 21% outsourced their digital forensic work, and investigating crimes against a company accounted for less than 20% of responses. Thirty-seven percent of respondents shared information on new trends in criminal acts or targets. Sharing or borrowing equipment accounted for about one-third of responses, while one-quarter of respondents needed additional personnel.

About half of these categories were based on “Other” responses from the previous year. However, notably, the number of respondents who said they relied on other organizations for advice declined from 75% to about 70% over the past year. Information sharing declined from 71% to about 55%. Trend-sharing declined from 49% to about 37%, while assisting with crimes against companies decreased by more than half.

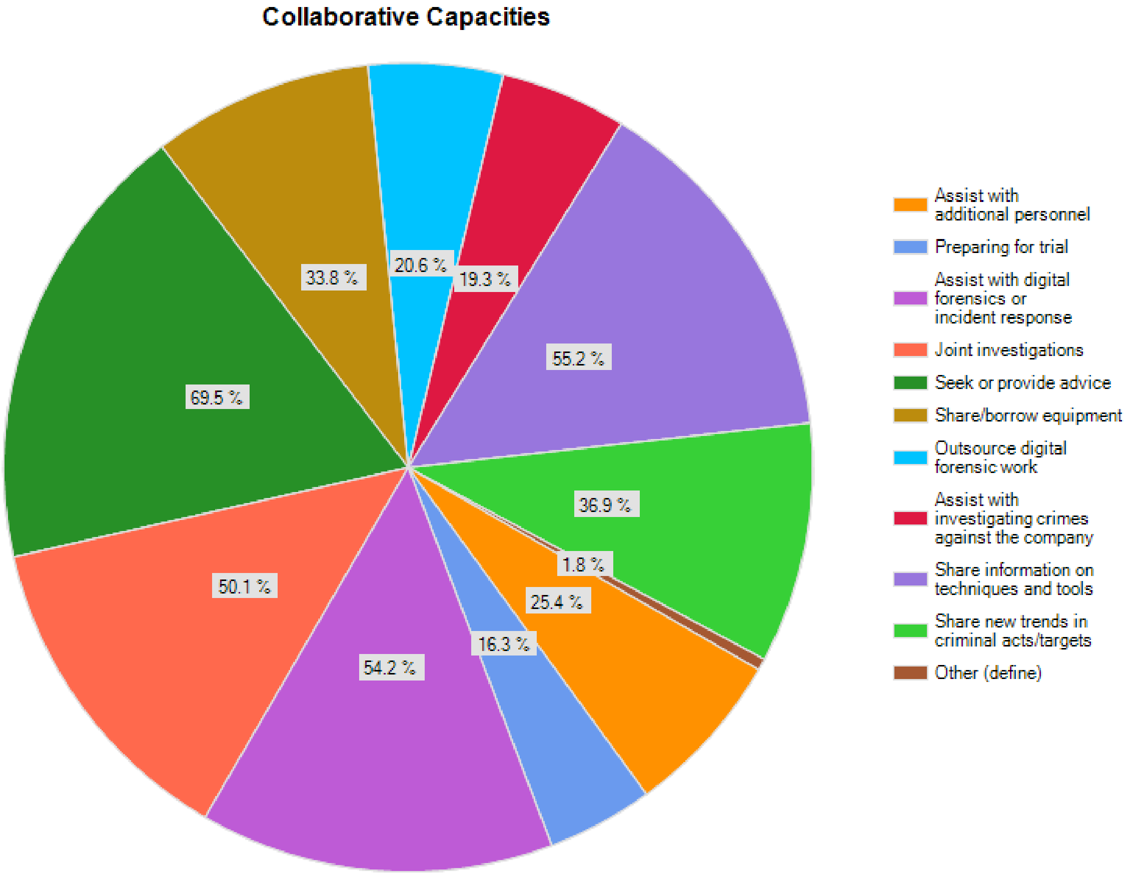

Figure 12- Collaborative Capacities

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 13, 14) Most respondents rated their cyber crime equipment at a 5 or a 7, but when it came to digital forensic equipment, most ratings were between 7 and 9. These are generally consistent with ratings from the previous year, although in 2011, both cyber crime and digital forensics equipment were rated somewhat more highly.

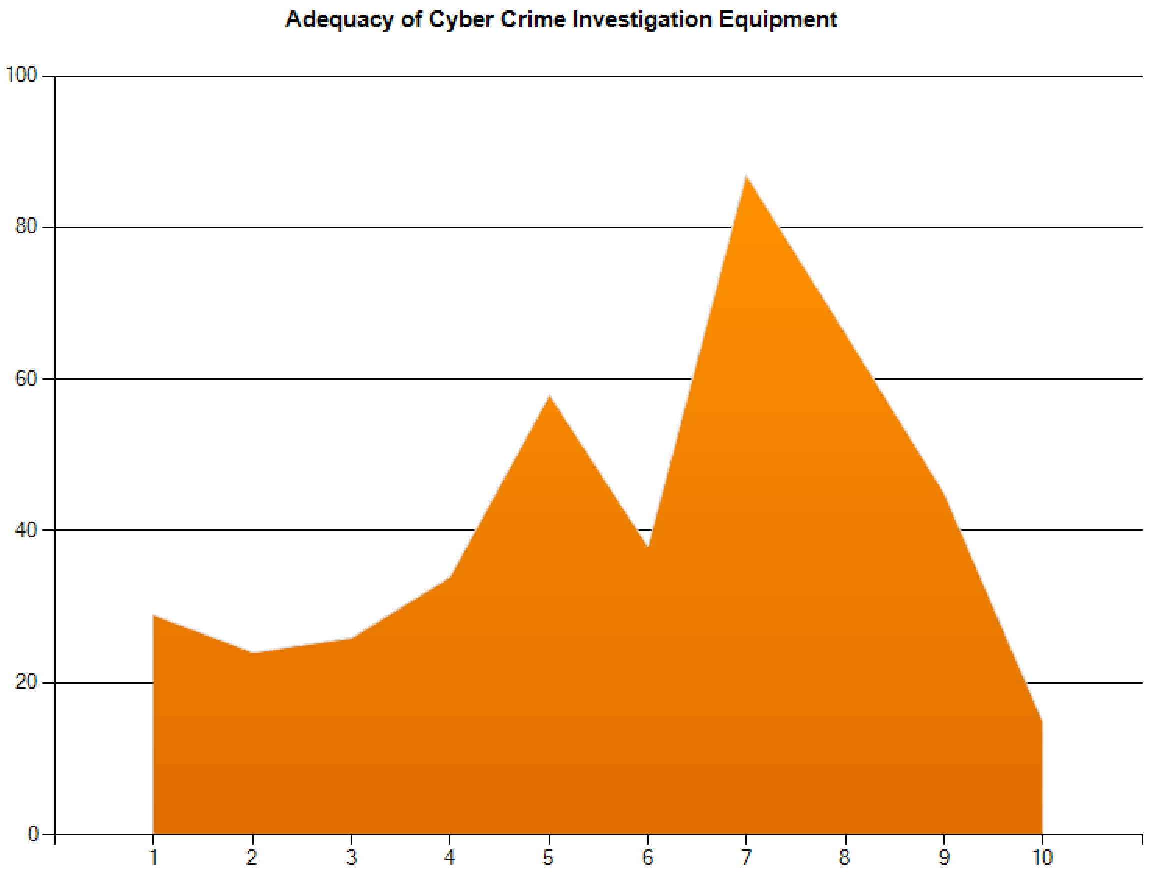

Figure 13- Adequacy of Cyber Crime Investigation Equipment

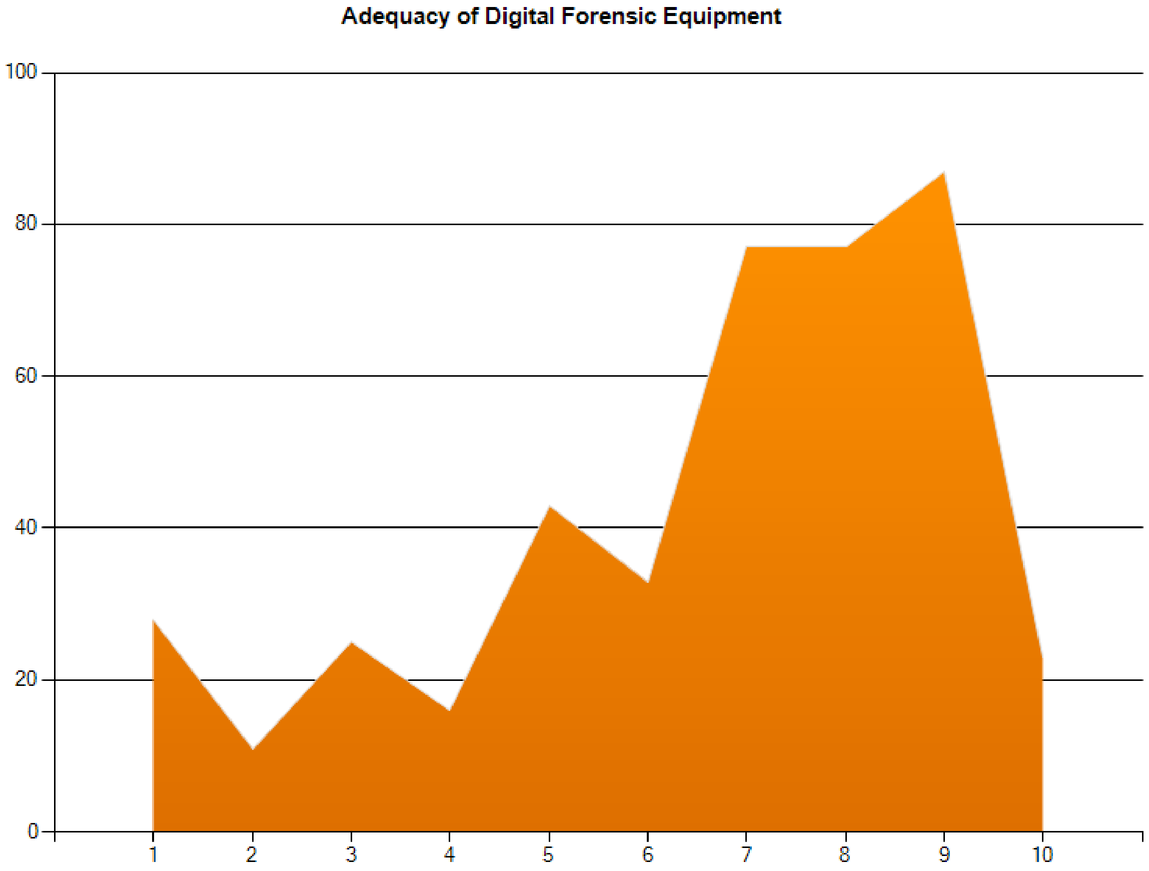

Figure 14- Adequacy of Digital Forensic Equipment

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-three percent of the respondents noted that their organizations spent more than $20,000 per year (a decline of 5% from last year); 19% said theirs spent between $1,000 and $5,000, another decline of about 6% from last year. The percentage of respondents who said their employers spent between $0 and $1,000 increased slightly (from 14% to about 17%), as did those who said between $10,000 and $15,000 was spent on equipment. However, declines were seen in all other categories.

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. About half each reported backlogs of less than six months, though digital forensic backlogs of 6 to 12 months were reported by almost 16% of respondents, compared with 10% who reported cyber crime investigation backlogs of the same time period.

More than one-third of respondents said they had no cyber crime investigation backlogs, while about 29% said they had no digital forensic backlogs. These numbers are roughly consistent from last year; the changes from one year to the next in the “0-6 months” category reflect that “Not backlogged” was a new choice this year.

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. Sixty percent said their organizations do take reports; slightly fewer reported that their organizations had a strategy for dealing with cyber crimes, and that their organizations had also set policies. These numbers were all lower from last year, but offset by the fact that “I don't know” was offered as a choice this year. An average of 12% of respondents chose this option for all three questions.

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 open-ended question, which allowed members to come up with subjective answers based on their own experiences.

This year, responses about technical and workload topics were very similar. Respondents were concerned about security issues and attack vectors, in particular malware; data encryption; more data on more (and larger capacity) media; cloud computing; and dealing with more technologically sophisticated criminals (and thus, crimes). Respondents also frequently mentioned globalization in context of working multijurisdictional cases, and the need for better proactive solutions as well as public education efforts. Some of these, such as encryption, were mentioned more frequently than last year.

As they did last year, many respondents also noted concerns with resources. However, where last year they most often mentioned the need for better, more affordable training, this year, resource mentions were more evenly distributed across budget, personnel, and training. The ability to convince management of the need for all three resources came up fairly often. Less often, respondents mentioned concerns with equipment and its ability to keep up with rapidly evolving technology. This year, a number also mentioned the loss of experience with investigator retirements, and the challenges of hiring and training replacement personnel.

Conclusions

Overall, responses to this year's survey were not drastically different from the responses to last year's. However, even marginal changes seem to reflect changes in the industry overall. For example, more respondents self-identified in the information technology, educational, prosecutorial and probation/parole fields than they did last year, and fewer respondents self-identified as being involved with digital forensics, incident response, corporate security or investigation.

This may indicate changes in overall HTCIA membership, as well as changes in member awareness and responsibilities outside the field in which they were trained. Either way, these and the other results indicate a need for better support in the following areas:

Information sharing and collaboration

An area of concern this year was the drop in the amount of time respondents spent collaborating with counterparts in other organizations. Decreases in collaborations with various types of organizations – task forces, other agencies, private companies, and so forth – could have been due to the greater range of choices offered in the question on this year's survey.

However, taken together with the following question – in which fewer respondents indicated weekly cooperation, and more respondents indicated none – the discipline of information sharing and collaboration may be suffering at a time when it is most needed.

Collaboration is the basic tenet from which HTCIA was formed, and within the investigative community, it is generally accepted that information and resource sharing is the key to success. On the other hand, the dynamics of information sharing are not well known, so it is more difficult to support the practice both for itself, and in situations where professionals may remain reticent even when they need help – for example, in situations where they fear bad publicity or when they lack the experience to be precise about their needs.

Future research should therefore focus on information and resource sharing among government, private, and academic organizations, both at home and abroad.

Public education

Public education in terms of Internet safety presentations was not rated highly; 42% of respondents ranked it only a 1 in importance to their work.

However, it is difficult to know whether this is because public education is not important to them, or because they don't have the resources to create, prepare for, and provide it. Standardized presentations and even curricula, such as HTCIA's Internet Safety for Children (ISFC) program, may help.

Another area that may fall under the “public education” mantle is computer and network security. With more respondents indicating that more training was needed in this area for both themselves and their colleagues, and also the high number of mentions of malware and other security issues in the last, open-ended question, associations and employers alike may wish to assist their members in providing security education to others.

Also, as last year's report noted, dedicated trainers may 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.

Organizational training

Training quality is still rated as being fair to good, and while training expenditures have decreased, they haven't been cut altogether. That few organizations use grant funding for training means this may be an area for them to explore further.

Also notable were the changes in percentages for each of the major training categories. Conferences remain a popular way to get training, but this year were ranked second behind chapter meetings – which in 2010 were sought by only 77% of respondents. This may indicate that rather than travel, more member respondents prefer to stay local.

However, because formal certifications and vendor training also ranked highly, chapters of associations such as HTCIA may want to work more closely with vendors to provide the kinds of credits their members seek.

Just as we found last year, 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.

Finally, responses indicate a need for training on how to document, explain and present digital evidence, not just in the courtroom but also to upper level and middle managers. This is borne out by the 29% of respondents who rated this job function a 10 in importance to their work, and also the many open-ended responses that spoke of the need to educate management on what they do.

Reporting, strategy and policy frameworks

Just as last year, 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 cyber crime 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
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