HTCIA

HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION

2013 HTCIA CYBERCRIME SURVEY

EXECUTIVE SUMMARY

OBJECTIVE

The objective of the 2013 Cybercrime Survey is to maintain an ongoing database allowing the HTCIA to track the changes in cybercrime investigations and training over a period of time. We invited individuals from numerous industries to participate and provide their insight on the current and future state of cybercrime investigations. The participants are members of local, state, and federal law enforcement and government agencies as well as those working in the private sector.

With this diverse sampling we are able to provide a valuable perspective on topics such as investigator tenure, department size and budget, training quality and opportunities, and caseloads and backlogs. The participants also shared with us the challenges they are currently facing and what they believe will be issues in the near future. The survey consisted of 40 questions and was open from September 2013 through January 2014. The 2013 survey includes the responses from 152 respondents.

2013 SURVEY RESULTS

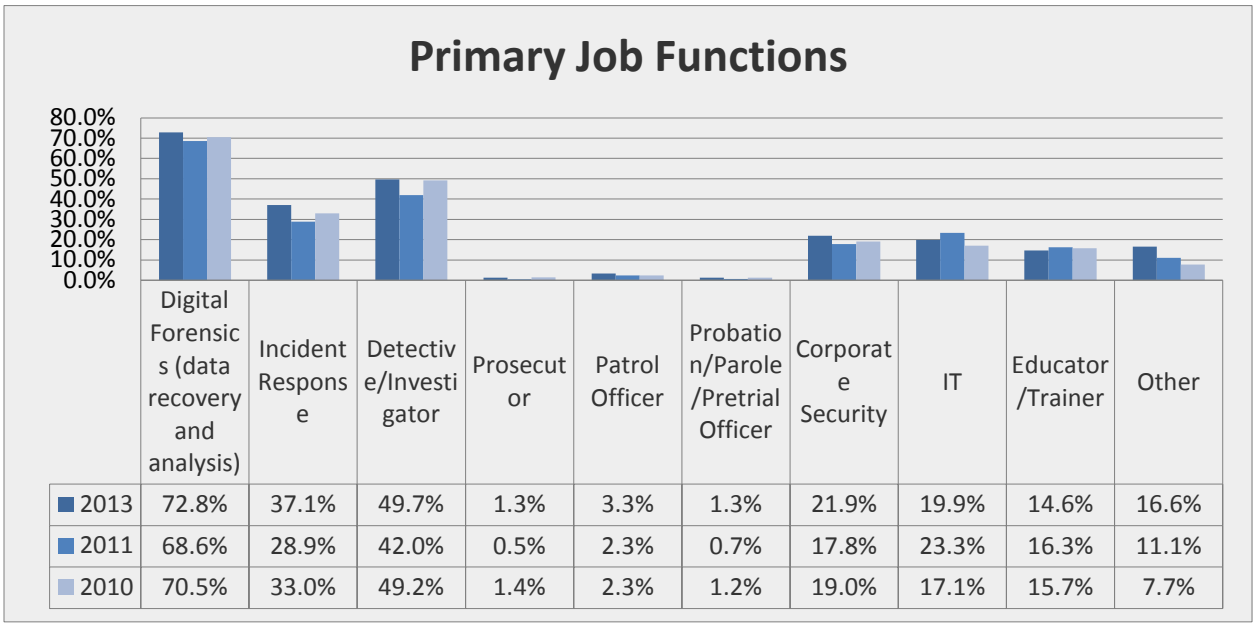
HTCIA MEMBERS Q1-3

Of the 152 participants, 141 people answered they are HTCIA Members and 11 people as non-members. All but 4 chapters had at least 1 member complete the Survey; the Silicon Valley Chapter had the most members complete the survey. Of the members that took the Survey, 37% have been members for less than 2 years, 34% with 3-7 years, and 30% who have been members for longer than 7 years.

JOB FUNCTION & EXPERIENCE Q4-10

When asked to describe their primary job functions 73% of people answered digital forensics (data recovery & analysis), 50% as detective/investigator, 37% as incident responder, 42% as IT/corporate security, 15% as educator/trainer. Almost everyone responded that they are involved with investigating cybercrimes: 58% people have more than 5 years of experience, 22% have between 3-5 years, and 14% with less than 2 years. The experience level is almost identical for those working on digital forensic

investigations: 57% have more than 5 years, 20% have 3-5 years, and 16% have less than 2 years experience.

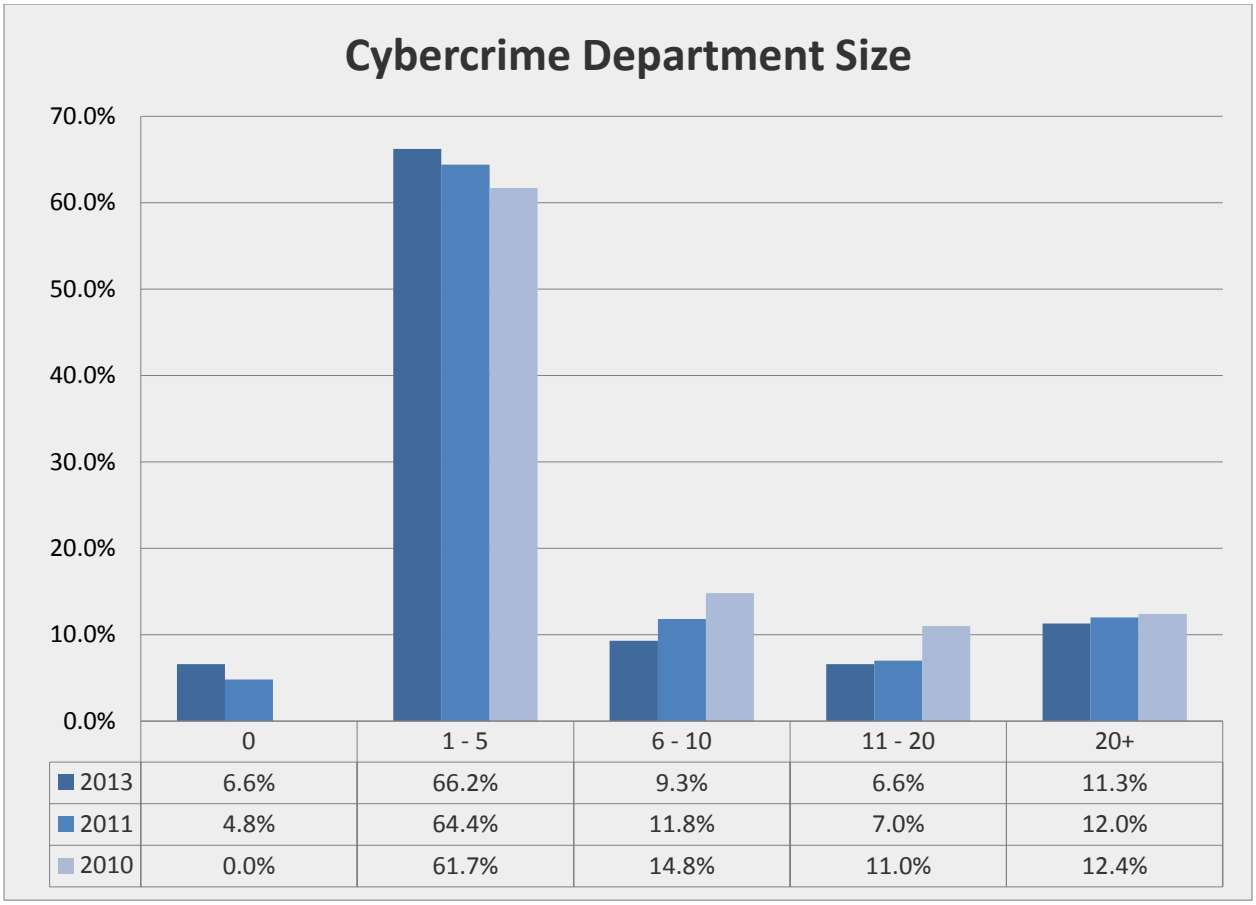


	Digital Forensics (data recovery and analysis)	Incident Response	Detective/Investigator	Prosecutor	Patrol Officer	Probation/Parole/Pretrial Officer	Corporate Security	IT	Educator/Trainer	Other
2013	72.8%	37.1%	49.7%	1.3%	3.3%	1.3%	21.9%	19.9%	14.6%	16.6%
2011	68.6%	28.9%	42.0%	0.5%	2.3%	0.7%	17.8%	23.3%	16.3%	11.1%
2010	70.5%	33.0%	49.2%	1.4%	2.3%	1.2%	19.0%	17.1%	15.7%	7.7%

Almost half, 49%, answered they are not involved with critical infrastructure security or investigations, 29% of people that do work in this field have more than 5 years of experience, and 22% people have less than 5 years.

Even fewer people are involved with e-discovery, 53% of people have no evolvement in this field, 21% of people that do work in this field have over 5 years of experience, 14% have 3-5 years, and 12% have less than 2 years experience.

When asked about their involvement with network security, 45% of people said they have no involvement in this area, 34% of people have more than 5 years experience, 13% have 3-5 years, and 9% have less than 2 years. Collecting, imaging, and examining digital evidence ranked as the highest daily priority for those that completed the survey. The lowest priorities were teaching, electronic monitoring, and critical infrastructure security & investigations.



	0	1 - 5	6 - 10	11 - 20	20+
2013	6.6%	66.2%	9.3%	6.6%	11.3%
2011	4.8%	64.4%	11.8%	7.0%	12.0%
2010	0.0%	61.7%	14.8%	11.0%	12.4%

INVESTIGATIONS & CRIMINAL/CIVIL TRENDS Q11-18, Q32-33

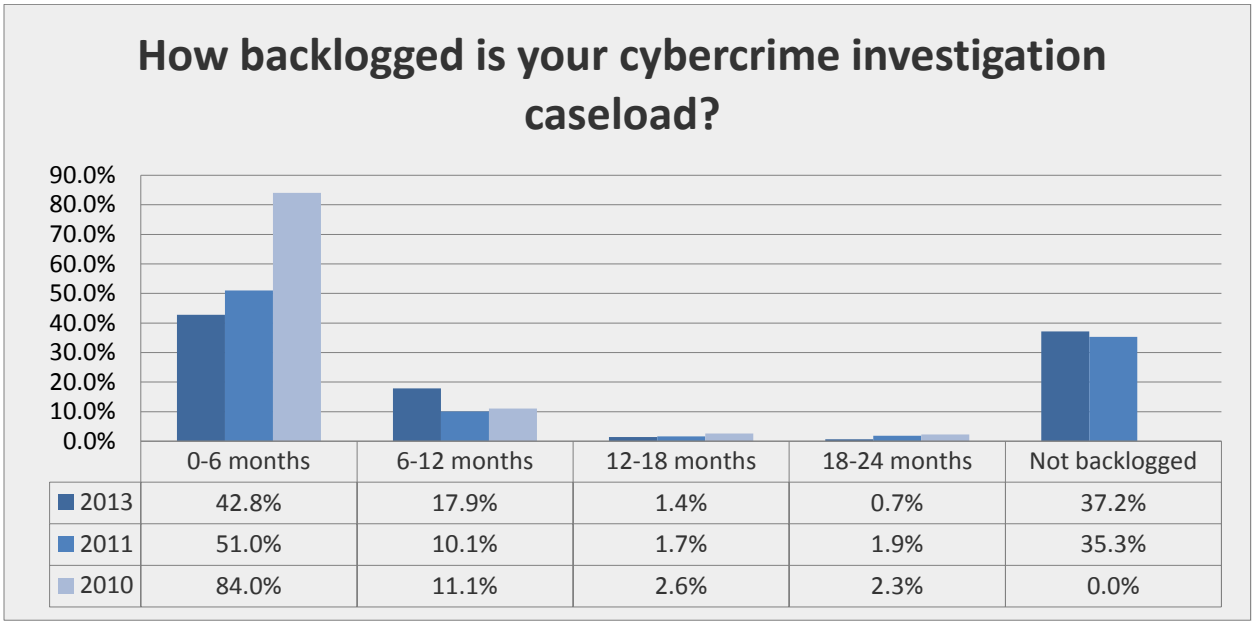
The prevalence of computer/Internet devices being used in criminal or civil offenses to: communicate with a victim, as an instrument in the offense, to record or keep track of a victim, or planning the offense has increased for about half of those surveyed, almost none saw a decrease, and about a quarter saw no change at all.

As far as specific criminal/civil offenses being investigated we saw the highest increase in fraud activity involving the Internet, identify theft, and credit card fraud. The majority of people working in the private sector saw an increase in corporate internal investigations. Almost no one saw a decrease in activity in any criminal/civil offense category most either saw no change or had an increase in activity.

The majority, 66%, of cybercrime investigator work in a small department staffed with between 1-5 people, 11% have 20 or more investigators working in their organization. Almost all of these positions are

considered full time; very few are part time or have other responsibilities within their organization. Critical infrastructure departments are also typically made up of small staffs, 43% have 1-5 people, 10% have more than 20 people, and 34% responded that zero people were working and/or responsible in their organization. Similar to cybercrime investigation departments almost all of the positions are full time with very little part time positions.

The majority of people's cybercrime cases are being worked in less than six months, 42% of people say their backlog is less than 6 months, 37% have no backlog, 18% are at 12-18 months backlogged, and only 2% have more than 18 months backlog. The digital forensics caseload is slightly more backlogged than cybercrimes: 41% of people said their backlog is less than 6 months, 30% have no backlog, 23% are at 6-12 months, 5% are at 12-18 months, and 1% are 18-24 months.



	0-6 months	6-12 months	12-18 months	18-24 months	Not backlogged
2013	42.8%	17.9%	1.4%	0.7%	37.2%
2011	51.0%	10.1%	1.7%	1.9%	35.3%
2010	84.0%	11.1%	2.6%	2.3%	0.0%

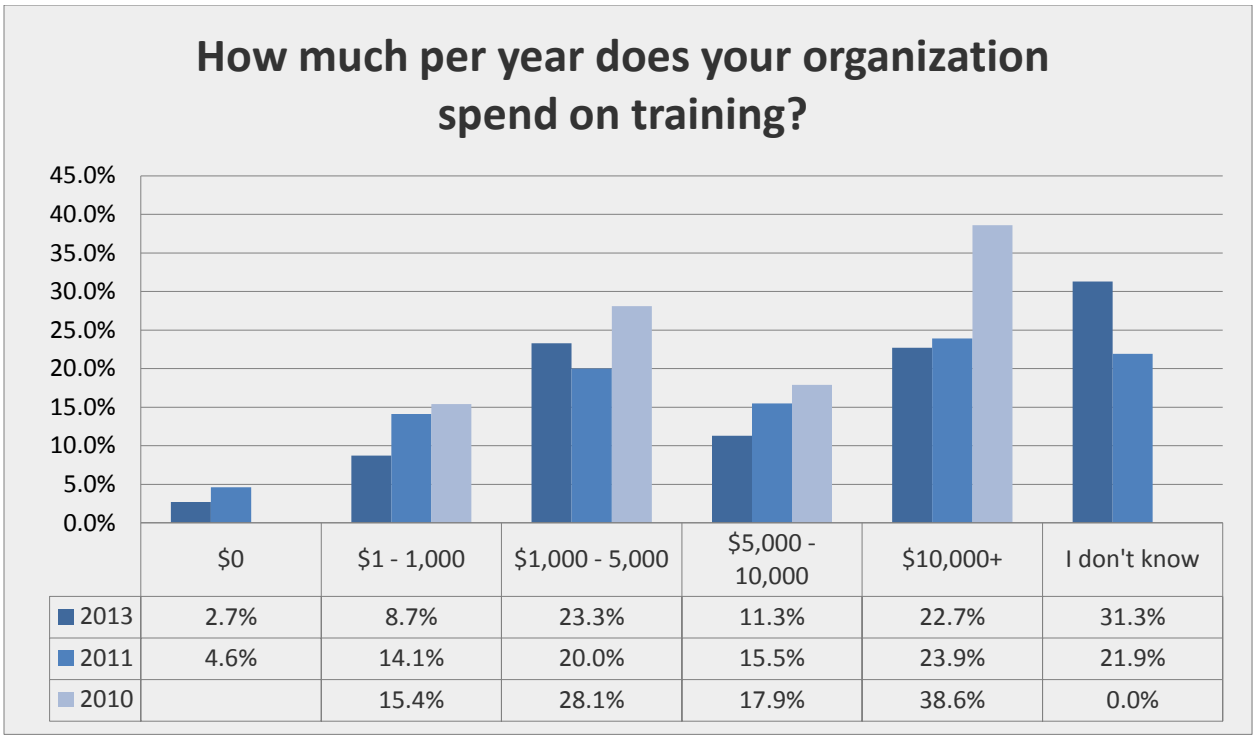
TRAINING Q19-25

When asked to rate the training they have received on a scale from 1 to 10, most people scored it in the highly satisfied range: 57% of people rated it as either a 7 or 8, 30% rated it between 4-6, and 6% rated it below a 3.

The majority, 58%, of people feel that other people in their organizations do not receive sufficient training on cybercrime investigations, 19% of people feel that other people were getting proper training.

The amount of money their organization spends each year for training was not known by 31% of people, 23% of people spend between $1,000-$5,000, 22% spend over $10,000, 10% spend less than $1,000.

Of the money spent on training 17% of people said they received funding from grants: 10% received between $1,000-$5,000, 4% received over $10,000, and 3% received $1-$1,000.



	$0	$1 - 1,000	$1,000 - 5,000	$5,000 - 10,000	$10,000+	I don't know
2013	2.7%	8.7%	23.3%	11.3%	22.7%	31.3%
2011	4.6%	14.1%	20.0%	15.5%	23.9%	21.9%
2010		15.4%	28.1%	17.9%	38.6%	0.0%

People are primarily looking to get training at conferences 90% or HTCIA chapter meetings 80%. Almost 80% are looking for formal certifications, free training, or vendor training. Less than half, 46%, are seeking training from blogs or podcasts and only 29% are looking for training through academic degrees.
Computer or network security is the number one area people would like to receive more training on, followed by online investigations, and then digital forensics. The least popular areas were Internet safety, electric monitoring, and undercover online investigations.

People would like to see others in their organization to receive training on collecting or imaging evidence, online investigations, and digital forensics. The least popular areas were Internet safety and electric monitoring.

COLLABORATION Q26-28

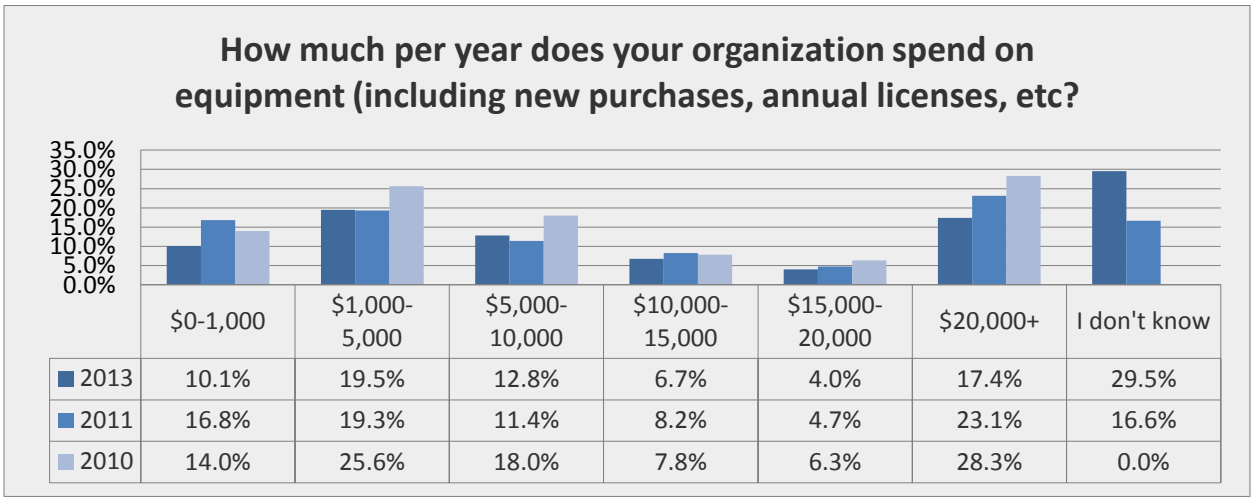
Almost everyone answered that they have collaborated with another agency/company during a cybercrime investigation, only 9% answered that they have never worked with another agency/company. Half of this collaboration occurs on a regular basis, 25% every month and 25% on a weekly basis.

Most people reached out to other local agencies, less than half from a private corporation or consulting firm, and very few from other government agencies or colleges and universities.
The top reasons for collaborating were to seek advice, share information on techniques and tools, and to assist with digital forensics or incident response.

EQUIPMENT Q29-31

When asked to rate the adequacy of their cybercrime investigation equipment on a scale of 1-10, a large portion rated their equipment very highly: 45% rated it as between 7-8, 28% rated it between 4-6, and 12% rated it below a 3. They are also asked to rate their digital forensic equipment on the same scale: 59% of people rated it between 7-9 and just 11% rated it below a 3.

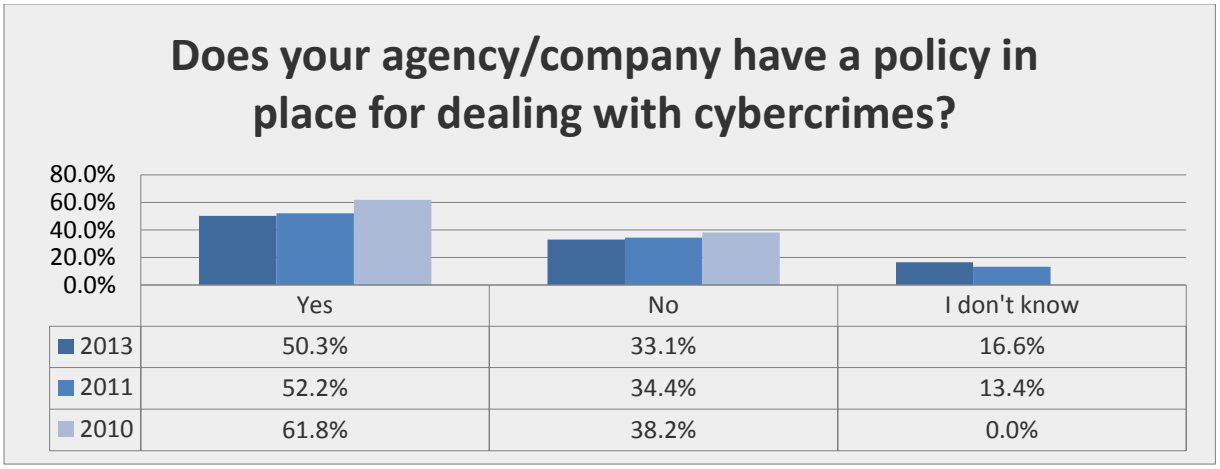
When it comes to cost per year on equipment: 30% of people do not know how much their organization spends, 19% spend between $1,000-$5,000, 17% spend more than $20,000, 12% spend $5,000-$10,000, 10% spend less than $1,000, 10% spend $10,000-$20,000.



	$0-1,000	$1,000-5,000	$5,000-10,000	$10,000-15,000	$15,000-20,000	$20,000+	I don't know
2013	10.1%	19.5%	12.8%	6.7%	4.0%	17.4%	29.5%
2011	16.8%	19.3%	11.4%	8.2%	4.7%	23.1%	16.6%
2010	14.0%	25.6%	18.0%	7.8%	6.3%	28.3%	0.0%

REPORTING & STRATEGY Q34-35

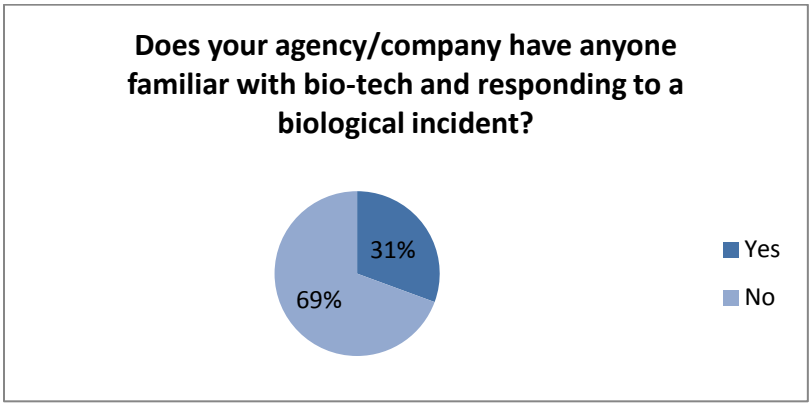
Many of the agencies and companies surveyed do take reports on cybercrimes: 59% said they do, 28% do not, and 13% were not sure. The statistics are about the same when asked if their agency/company has a strategy to deal with cybercrimes: 58% said they do, 25% do not, and 16% do not know. But only 50% said there is a policy in place for dealing with cybercrimes, 33% do not have a policy, and 17% do not know if there is a policy.



	Yes	No	I don't know
2013	50.3%	33.1%	16.6%
2011	52.2%	34.4%	13.4%
2010	61.8%	38.2%	0.0%

BIO-TECH Q37-38

Very few people, 31%, have someone at their agency/company that is familiar with responding to a biological incident. If training were offered for bio-tech incident response 60% said they would be interested in participating, 40% said they would not be interested in training.



TOP 5 CYBERCRIME CHALLENGES OVER NEXT 12 MONTHS Q39

We asked what the top 5 challenges cybercrime investigators are facing over the next 12 months. This was an open question and no specific answers were listed.

As most would expect, people's biggest challenge is working with smaller budgets or having no money at all, this issue has a wide reaching impact on cybercrime investigations. Without proper funding people are having difficulties keeping up with their caseloads due to staffing cuts or they are not able to bring in additional personnel to help with an increasing caseload. They are also not able to attend training classes/events, which is making it difficult to keep up with the advancing technology, new or improved methodologies, and criminal/civil trends. Without the necessary money in their budgets people are having to reduce spending on equipment/software, this is leaving some with outdated equipment/software or preventing them from being able to expand their labs to handle increasing caseloads. With the increase of bigger and bigger hard drive/device sizes and storage space people are having a hard time getting the equipment they need to quickly image and process these large data cases. Training is also being reduced or eliminated because there is no longer any money to attend training classes or conferences, which is then reducing the amount of qualified and experienced investigators in their organizations. Salary and compensation have also been negatively affected by budget cuts.

Training and development, aside from funding issues, was also a common challenge people are facing. Respondents felt like there was a lack of training available for new investigators, especially in law enforcement was people with no experience are promoted into forensic/cybercrime departments. With technology rapidly advancing and ever changing, investigators feel like training for new technology/devices is not keeping pace; they would like to see training classes update their material faster and offer classes specific to new technology/devices. Career development training, for both law enforcement and private sector, is also an area people feel is lacking and needs improvement. Network security, malware, incident response, and cloud storage were major areas that investigators felt that they need additional training as their caseloads are now expanding into these fields. As new laws are passed and existing ones challenged/overturned the need for legal training is needed to keep investigators informed on issues such as proper evidence/information gathering or obtaining warrants and subpoenas. Mobile device training was another area investigators felt like they needed more training on as well as the need for training classes to stay current/update with new devices entering the market. There is also a need for training on big data processing to help reduce the amount of time it is taking to work these types of cases.

Another major challenge being faced is a lack of understanding/knowledge for digital forensics and cybercrime by executives, commanders, general public, prosecutors and judges. Many people expressed that the higher ups in their organization do not understand the current or future landscape of cybercrime

and forensics; this is holding departments back and preventing them from being able to keep pace with current trends. The general public's lack of awareness and education with regards to cybercrime is contributing to higher caseloads, as they are falling victim to scams or attacks. The individuals in legal system are also in need of training, prosecutors and judges do not have the necessary knowledge needed to understand the increasingly complex cases, which can affect how or if a case is prosecuted and potentially how a jury decides the verdict in a case.

Cybercrimes often crosses multiple jurisdictions and international borders; this can slow down or even prevent investigators from stopping criminal/civil offenses or bring the offenders to justice. Investigators view the lack of or limited collaboration with foreign agencies as a major challenge when fighting cybercriminals who are able to take refugee overseas and likely never be held accountable for their offenses. There is also a need for a more streamlined process for collaboration with other local, state and federal agencies when investigating cybercrime that crosses multiple jurisdictions. Those in the private sector would also like to have a more streamlined approach when working with law enforcement on criminal cases against their organization.

IMPROVING SURVEY Q40

The top suggestion for improving the survey was to break it into two surveys; one survey for law enforcement and one for the private sector, so that the questions can be tailored for each group, as well as the ability to compare the responses. Other suggestions included having an incentive for completing the survey and some minor wording changes to a couple of questions.

ABOUT THE HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION (HTCIA)

"INVESTIGATORS ON THE LEADING EDGE OF TECHNOLOGY"

The High Technology Crime Investigation Association (HTCIA) was formed to provide education and collaboration to our global members for the prevention and investigation of high tech crimes. As such, we are an organization that aspires to help all those in the high technology field by providing extensive information, education, collective partnerships, mutual member benefits, astute board leadership and professional management.

The HTCIA's mission is to provide education and collaboration to our global members for the prevention and investigation of high tech crimes. Its core purpose is to promote collaboration and education of our members.

HTCIA, Inc.
3288 Goldstone Drive
Roseville, CA 95747
(916) 408-1751
(916) 408-7543 Fax
http://www.htcia.org

For public relations information, please contact Carol Hutchings – carol@htcia.org

REPORT PREPARED BY:

MATTHEW SNYDER
PETER MORIN
CAROL HUTCHINGS
ELISA HUTCHINGS