**Project on Cybercrime**

Version 1.0 – 9th March 2009

Study
Co-operation between LE, Industry and Academia
to deliver long term sustainable training to key cybercrime personnel

# 2CENTRE

**C**ybercrime **C**entres of **E**xcellence **N**etwork for **T**raining, **R**esearch and **E**ducation

Prepared by
Cormac Callanan (Ireland)
Nigel Jones (UK)

This report has been prepared within the framework of the informal Law Enforcement – Industry working group hosted by University College Dublin.

## Contact

For further information please contact:

**Cormac Callanan**

Tel: +353 87 257 7791

Email: cormac.callanan@aconite.ie

**Nigel Jones**

Tel: +44 7786 317995

Email: nigel.jones@technologyrisklimited.co.uk

This study does not necessarily reflect official positions of any of the external contributors or of the donors funding this project

 

## Contents



 

# 1 Executive Summary

This study examines the current methods of training law enforcement and industry in IT forensics and cybercrime investigation. It reviews the activities undertaken by members of law enforcement and relevant industry personnel to gain knowledge and skills in an area which currently has a diverse range of levels of professional training, in-house training, cross training and on-the-job learning.

Law enforcement has insufficient training options in IT forensics and cybercrime investigations and in Europe generally rely on courses provided by Europol and/or Interpol. In addition, a number of countries have developed their own law enforcement cybercrime training programmes either alone or in conjunction with academic institutes. Law enforcement has also been provided with and availed of a large number of training courses, seminars, conferences and hands-on training provided by different industry players in locations throughout the world. These methods are not proving to be scalable or sustainable, nor do they follow a training path or provide a standard assessment of knowledge or competence. Currently, it is difficult to measure the usefulness and effectiveness of these efforts. Current international cross-coordination of training activities is limited and relies on a few individuals to drive the activities.

Both groups of actors – law enforcement and industry – have arrived at the realisation that ad hoc training provided on request or as part of ongoing but irregular support services do not provide sustainable, scalable, standards based, measureable skills delivering the requirements of the cybercrime forensics investigator today.

Industry also realises that skilled internal security professionals with experience in IT forensics are very difficult to recruit and train and therefore also require personnel already trained in a similar manner to law enforcement personnel – with minor variations. Concerns on the part of law enforcement have so far limited the opportunities for industry to avail itself of the training and qualifications on offer to law enforcement. Training for industry is also needed by legal and IT personnel of service providers who deal with law enforcement daily and answer to law enforcement requests

In order to continue the development and delivery of effective cybercrime training to law enforcement on an international level, it is necessary for them to partner with learning organisations and industry to create a network to take responsibility for the programmes and academic oversight, and where possible, offer of appropriate academic qualifications.

These academic institutions are in a position use their considerable pool of research and education expertise to support both LE and industry in the development of education

 

programmes designed to facilitate the enhancement of skills and qualifications relevant to the area of cybercrime.

In 2006 University College Dublin, Ireland established the UCD Centre for Cybercrime Investigation with the creation of a state of the art forensics laboratory and the development of a Law-Enforcement-only Masters degree in Forensic Computing and Cybercrime Investigation. To support ongoing education & training development, administration, and delivery, the university currently provides funding for five full time staff in the centre as well as the ongoing use of the premises. UCD's MSc in Forensic Computing and Cybercrime Investigation (MFCCI) is an accredited programme specifically designed in partnership with law enforcement. The programme is run on a not-for-profit basis and is currently restricted to law enforcement officers.

The conclusion of this review is the immediate need to support and develop ***Centres of Excellence*** which provide academically accredited training in a modular format developed in cooperation with law enforcement and industry targeted at the cybercrime forensics investigator or in-house IS security. This may be achieved by creating Centres of excellence that meet certain criteria. An example of the way in which such cooperation may work can be seen within the series of "Cybercrime training" projects run under the auspices of the European Commission Falcone and Agis programmes.

The development of education provision that is academically accredited and specifically focused on the delivery of skills to support both the LE investigator and industry in-house security personnel can be designed in collaboration with stakeholders from those organisations to ensure that content is appropriate to requirements.

The centres should strive to define research topics and programmes, master and doctorate thesis topics and establish cybercrime research as a recognized legitimate research area. This would in turn would help attract talent to the various stakeholders (LE, industry, academic centres), and complementary funding (from research funding agencies such as the French ANR, industry, or even European Commission programs). The centres of excellence network's own funding and skills would in the end find considerable leverage.

These Centres of Excellence, which can be located throughout Europe and the world, should work together in a Network of Centres of Excellence to ensure minimum duplication of effort, high quality training and research, shared with others in the network to ensure consistency and scalability compatible with cultural and linguistic sensitivity. This will enable the realisation of a sustainable programme of training across international borders leading to certifications and qualifications that accommodate learning in different jurisdictions.

It is recognised that the international policing organisations involved in cybercrime training activities are limited by budgets and resources in the number of events that can manage each year. Europol for example is an operational organisation and holds one training course a year in a cybercrime related subject. Interpol holds 2 cybercrime training courses a year in Europe and has a training skills development programme to supplement the low number of effective trainers in this field. Training is not the major role of these organisations and although their efforts are worthy, they will also benefit from the creation of a network of Centres of excellence in which they can play a full part without burdening them with administrative overheads.

The creation of a network of Centres of excellence will require coordination and it is proposed that a ***network coordination centre*** be appointed to undertake this role. The network coordination centre would strive to find the right balance between the flexibility required by the networking of the Centre's and the achievement of a concrete knowledge base that could be transferred to new Centres. The network coordinator would seek the close engagement of key trans-national stakeholders in law enforcement (e.g. Council of Europe, Europol, Interpol, OSCE, and UNODC, Asia-Pacific Economic Cooperation (APEC), Association of Southeast Asian Nations (ASEAN), Organization of American States (OAS) and in industry. (E.g. EuroISPA, intellectual property groups, etc)).

The network coordination centre would focus on five key areas:

- Encouraging excellence in each Centre.
- Expanding the network to support new Centres and new countries as appropriate
- Supporting external relationships with trans-national agencies and activities
- Promotion of the work of the Centres and the network
- Working with the proposed ISEC project team to further develop the programme

The network coordination centre and each Centre of excellence would establish an ***advisory board*** which would involve relevant stakeholders from law enforcement, industry and academia to provide oversight and guidance of the strategy of the organisation. It is essential in the early stages that the network coordination function includes participants from industry, law enforcement and academia and should seek to build on the knowledge gained from the aforementioned Falcone and Agis projects as well as the work of the Europol Working Group on the Harmonisation of Cybercrime Training.

At the June 2008 meeting of the Europol Working Group on the Harmonisation of Cybercrime Training, it was proposed that a bid be submitted under the framework partnership of the ISEC EC funding programme to develop a Centres of Excellence project. The

 

recommendation of this study is to submit a bid to establish, operate and develop a ***Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE)*** to the EC funded ISEC programme.

The network coordination role is seen as *a critical element* to the overall project and the sustainability of the network at the conclusion of the project. 2CENTRE would start with a network coordination centre with a small number of dedicated personnel who are neutral and separate from, but working with, the initial Centres of excellence. This network would initially consist of an Irish Centre of excellence based in University College Dublin and a French Centre of excellence based in Université de Technologie de Troyes. As a group. the network would develop rules and procedures and best practice to enable others to '*qualify'* for membership of the network on equal terms with other members. Experience has shown that a network such as this will have limited success without dedicated personnel since the Centres of excellence will need to focus all their resources on the development and delivery of education. The international coordination of this work performed by the network coordination centre both internally and externally will reduce the duplication of effort and ensure rapid smooth expansion of the network to other regions and languages.

For such a new domain, EC support would be necessary to help the network coordinator in self-organisation and to raise awareness to involve the main stakeholders. Additional support from industry would be essential. It is envisaged that new members would be invited to join the network and it is anticipated that law enforcement agencies, industry and academia would join or cooperate with the initial Centres during the ISEC project to allow the developed systems to be tested before the completion of the project. The network will be allowed to expand further at the conclusion of the project and the final report to the European Commission is submitted and made available to partner organisations and interested parties.

# 2 Introduction

## 2.1 Scope

Following the Industry meeting held at UCD, Dublin on 1st - 2nd October 2008, it was decided that further information is required in order to progress the issues raised at the meeting, with a view to producing a paper to be delivered at the Council of Europe Cybercrime Conference on 10 -11 March 2009.

The focus of the report will be to garner support from law enforcement and industry executives to support the recommendations of the report.

The scope of the paper is as follows:

- Background
  - Current initiatives
  - Summary of the state of cybercrime training and qualifications currently available to Industry and LE (including academic and competence based activities)

- Gather information from law enforcement regarding
  - current training delivered to industry
  - currently available qualifications
  - Currently available competency based certifications
  - Details of standards that apply to the area of digital forensics and cybercrime investigations and their relationship to points 3.1, 3.2 and 3.3
  - What LE knows about the Industry training requirements
  - Current training delivered by industry to law enforcement
  - The law enforcement requirement for cybercrime/investigation training

- Gather information from industry regarding
  - current training delivered to LE and the cost where known
  - What industry knows about the LE requirement for this training
  - Currently available qualifications for industry
  - Currently available competency based certifications for industry
  - The industry requirement for cybercrime/investigation training

- A vision for the future of cybercrime training for LE/Industry incorporating:
  - Methods of delivering training
  - Centres of Excellence
  - Collaboration between LE/Industry/Academia
  - Funding opportunities (e.g. European Commission programmes)
  - Standards and good practice
  - International qualifications
  - Continuing professional development
  - Examination of the possibility for joint training initiatives

## 2.2 Structure of the Study

Nigel Jones and Cormac Callanan will produce the paper. They will gather the required information, produce a draft report and take feedback from those present at the meeting in Dublin.

The report will be presented in session during the Council of Europe Octopus Conference in Strasbourg in March 2009

## 2.3 Why create the study?

Organisations are constantly developing support services for new and existing personnel. As part of this there is a need for training programmes for personnel to equip them with the knowledge and skills necessary to ensure their work related skills and activities are matching international standards.

The main purpose of this study is to identify ways in which the relevant stakeholders and others can be more effective in developing and delivering cybercrime training to law enforcement globally. They study will also examine the requirements of industry with regard to training and qualifications for its staff and how academia and law enforcement my support that effort.

Bidirectional Communication[1]

Systematic analysis of the structures of current cooperation shows, that it is bidirectional in nature:

- Law Enforcement is on the one hand responsible for the prevention and investigation of crime and on the other hand knowledgeable on cybercrime trends.
- Computer and Internet industries are on the one hand victims of crime and on the other hand knowledgeable about some cybercrime trends and hold data about their customers who are perpetrators or victims of criminal acts. They also hold valuable information about their products that is useful to law enforcement in its fight against cybercrime

An effective fight against cybercrime therefore requires a carefully considered approach from industry and law enforcement. With the complexity and speed of development of new technologies such as new services being offered online for free, Service Providers are increasingly being asked to engage in a more active way in addition to responding to requests from law enforcement. Law Enforcement does not have the capacity to develop

[1] Council of Europe Project on Cybercrime, Study of Cooperation between service providers and law enforcement against cybercrime (www.coe.int/cybercrime)

 

internally all the expertise which is required and cooperation with the private sector is not necessarily something done routinely. Law Enforcement can gain and maintain an understanding of new technology areas from the Computer industry and Internet Service Providers. Industry and Law Enforcement need to share their expertise and concern.

Historically there has been limited official cooperation between law enforcement and industry in the development of training and capacity building to combat the threat of cybercrime. Law Enforcement agencies in different jurisdictions have traditionally developed their own training programmes and in some instances have worked with industry and academia in order to meet short term national objectives.

Since 2002, a coordinated effort has been made to harmonise cybercrime training across International, and in particular European borders. This has involved EU countries working together in pursuit of a concept developed in an EC Falcone funded project entitled **'***Cybercrime Investigation – Developing an international training programme for the future*"

That project identified a route for the development of a training programme linked to academic accreditation which was implemented in subsequent European funded programmes that developed and delivered training courses in all EU countries and made the training material available to Law Enforcement on a global basis.

The programme has been developed as collaboration between law enforcement and academic institutes and has led to the creation of a *Master of Science in Forensic Computing and Cybercrime Investigation* award that is currently restricted to Law Enforcement. This restriction is primarily due to the fact that the taught modules were initially developed with European Commission funding that restricts the output to non profit law enforcement use. However, the Masters has evolved considerably since its inception and now consists of independently developed content designed within the University itself.

Since 2006, industry partners have joined the projects and it has become apparent that in addition to the law enforcement requirement for training, industry has its own cybercrime training needs that are not currently being met in a coordinated manner.

Closer collaboration between industry, law enforcement, academia and international organisations has been possible primarily through the formation of the Europol Working Group on the Harmonisation of cybercrime training. In addition; collaboration between Microsoft and Interpol has created a global law enforcement training programme coordinated by the International Centre for Missing and exploited Children (ICMEC) based in Virginia, USA.

 

It is apparent that there are a number of industry organisations that have law enforcement support programmes yet these are uncoordinated with other industry and law enforcement programmes. The effect of this is that individual fragmented efforts provide little measureable long term benefit to the recipients of that support or the overall fight against cybercrime

The economic downturn has emphasised the need to work in a smarter way and this study identifies ways in which the key partners in law enforcement, industry and academia can provide a more effective approach to delivering much needed training to law enforcement, provide a better return on available resources and also meet the needs of industry in developing their knowledge and skills in an environment that will also lead to appropriate qualifications.

This study firstly provides an overview of different programmes that currently operate, secondly outlines the needs analysis of law enforcement and industry for cybercrime training and finally makes recommendations how a comprehensive, flexibly, coordinated approach will deliver consistent, targeted, reliable and repeatable training to students from different background and cultures. This training will have the key objectives of being sustainable, standards based, scalable and its effectiveness will be measureable.

# 3 Background

## 3.1 Current initiatives

### Law Enforcement Initiated

The Europol sub group on the harmonisation of cybercrime training born out of the successful European Commission funded projects is probably the best known example of the development of training programmes for the law enforcement community, created by collaboration between Law Enforcement, Academia, Industry and International Organisations. The group has a five year plan for the development, maintenance and delivery of cybercrime training and qualifications. The current project has some 30 partners from these groups and is seeking further funding to develop more advanced training in line with the threats of cybercrime.

Interpol through its five regional working groups is delivering training and capacity building in all parts of the world. It is a partner in the Europol initiative and utilises the training material and other resources from the partners in the European project.

There is a strong working relationship between Law enforcement and industry in the Asia Pacific region with tools developed by industry being made available to law enforcement on a global basis. There are other joint initiatives that relate to specific investigations such as those involving Botnets and facilities made available by industry to support law enforcement activities.

It does seem that most of the initiatives involve industry as donors and law enforcement as recipients. The study should identify whether it is possible for law enforcement to provide training to industry.

One area that has not been fully explored is the possibility to use the partnerships that may be developed to provide an investigative support capability to be taken advantage of in cases of major international cyber incidents. Traditionally LE has tended to focus on individual crimes, however given the likely increases in incidents such as widespread denial-of-service attacks which recently occurred in Estonia, it might be useful to mobilise the corps of partners. This area is considered as relevant once the relationships have been formed to develop the training, education and research functions and is not dealt with any further in this paper.

INTERPOL, which has worked to train law enforcement officers around the world and to date, has established various Working Parties on Information Technology Crime in Europe, Asia-Pacific, Africa, North Africa/Middle East and the Americas regions. While much training has been given, it has been thus far on an ad hoc basis, and thus not formally linked to any

 

certification or qualification process. Many other multi-lateral organisations have also engaged in cross-regional training projects, including APEC, ASEAN and the OAS. As noted with Interpol, much of this training was ad hoc in nature and did not provide an ongoing level of instruction culminating in any official certification or qualification.

It is important that any proposed model for future cooperation takes account of the fact that many of the cyber crime threats posed to the European Union emanate from beyond the EU's borders, it is critical that European law enforcement officials build solid relationships with their counterparts in other regions of the world. Not only is this logical from an investigative and operational perspective, but also from a training perspective as well.

One such organisation with whom cooperation might be desirable is the International Multilateral Partnership Against Cyber Threats (IMPACT), located in Kuala Lumpur, Malaysia. IMPACT has been designated by the UN's International Telecommunications Union as the key organisation to implement the UN's Global Cyber security Agenda and as such has responsibility for coordinating cyber crime and terrorism incidents in 191 countries around the world.

IMPACT has established a Global Cyber Response Centre to deal with real-time emerging cyber threats. In addition, it has a large academic network of over 20 universities spread across the globe conducting research on cyber security and assurance. While IMPACT is not specifically focused on the law enforcement community alone, it does provide a model to bring together law enforcement, regulators, governments, academic institutions and the NGO community to respond to the common threat posed by cybercrime and terrorism.

As part of the work proposed herein for the European Union, this study sought to identify appropriate partners such as IMPACT with whom we can cooperate to ensure that the work of the EU and other international initiatives is appropriately shared and harmonised across regions.

**University College Dublin**
**MSc in Forensic Computing and Cyber Crime Investigation**

It is now accepted that LE officers involved in cybercrime investigation around the world should be educated to the highest possible level. If possible, they should obtain formal accreditation for such education which enhances their standing when providing testimony in the courts.

In 1997, University College Dublin's (UCD) helped to develop a 1 year Certificate in Forensic Computing and Network Security for the Irish Garda Computer Crime Investigation Unit to enhance their ability to combat technology related crime. This programme operated for three years and delivered targeted technical education to Law Enforcement personnel. UCD also

 

provided pro bono expert assistance in criminal cases at a time when LE was establishing their skills in cybercrime.

In 2006 UCD established the UCD Centre for Cybercrime Investigation (UCD CCI) with the creation of a state of the art forensics laboratory and the development of a Law-Enforcement-only Masters degree in Forensic Computing and Cybercrime Investigation (MSc FCCI). The MSc FCCI was initially developed using the material created through the AGIS projects and was designed to address one of the goals of the initial FALCONE report that identified a requirement for advanced LE qualifications in the field. To support ongoing education & training development, administration, and delivery, the university currently provides funding for two full time staff in the centre as well as the ongoing use of the premises required to house the UCD CCI.

UCD's MSc in Forensic Computing and Cybercrime Investigation (MFCCI) is an accredited programme specifically designed in partnership with law enforcement. The programme is run on a not-for-profit basis and is currently restricted to law enforcement officers. The programme is being continually revised and updated in order to remain up to date in relation to cybercrime threats and makes constant use of research undertaken in the University to support content development.

Since its establishment over 60 LE officers from 15 countries have graduated or are currently participating in the programme. The course is designed as an online learning programme to allow working professionals to learn in their own time and at their own pace.

In addition to supporting European and Europol initiatives, UCD Centre for Cybercrime Investigation participates as a member of the Irish Delegation to the INTERPOL Working Party on IT Crime – Europe. Membership of this group has led to the centre being asked to assist INTERPOL in a variety of ways:

- Interpol requested the UCD Centre to design a training programme[2] that would support LE officers in becoming trainers in their own right. This was a capacity building initiative that would facilitate the expansion of skilled cybercrime investigators in regions where they were most needed
- UCD CCI has been requested by Microsoft and INTERPOL to act as validators for the COFEE forensics tool. Experts from CCI are currently testing the tool, and a training pack is in the process of being developed
- In May 2008, UCD CCI was requested to and agreed to provide expertise to

[2] The course was piloted in India in March 2008 where 20 LE officers from the South East Asia region attended a programme that provided a combination of both technical and soft skills training. This course was delivered again in Cyprus during January 2009 and supported on a pro bono basis by UCD CCI in providing trainers for the event. Further courses are scheduled for other regions later in 2009

 

participate in a meeting to review the outcomes of an operation conducted by Interpol in relation to the seizure of computers, belonging to the FARC terrorist group, by Columbian authorities

- Interpol collaborations with UCD Centre for Cybercrime Investigation have led to the creation a Memorandum of Understanding between the two organisations to be finalised in April 2009. A further Memorandum of Understanding is to be completed between the International Multilateral Partnership Against Cyber-Threats (IMPACT) and the UCD Centre for Cybercrime Investigation.

UCD Centre for Cybercrime Investigation is also collaborating closely with the Organization for Security and Co-operation in Europe (OSCE), and is currently organising an LE training programme due to take place in Serbia later this year.

**Université de Technologie de Troyes**

A specific collaborative effort has been undertaken in France that has led to an LE/Academic relationship. In 2001, the Gendarmerie Nationale launched at its "*National centre for judiciary police training*" (CNFPJ) in Fontainebleau the first training of specialised investigators (who are called "NTECH" in the gendarmerie). This 4 week training program evolved over the years up to 6 weeks of training, covering high tech legislation, investigations, forensic analyses of computers, mobile phones and smart cards as well as relations with industry.

Currently, industry is invited to participate in the NTECH training. This includes presentations by a French ISP, the three French GSM companies, the French ISP association and a French content producer (Canal+), etc,. The feedback goes in both directions and these training sessions are very much appreciated.

Every year, the police and the gendarmerie organise a joint seminar for their specialised investigators (NTECH for the gendarmerie and ESCI for the police). Industry is regularly invited to make technical presentations.

In 2005 a partnership was signed with the Université de Technologie de Troyes to obtain academic accreditation of this training, which has now become a "university diploma", which covers a year of training (5 weeks in class at the CNFPJ, 3 weeks in classes at the UTT and the rest of the year devoted to personal work and the preparation of a small thesis on a technical or investigative topic.

Since 2006, 5 selected among experienced "NTECH" have access each year to a master degree training at the UTT on information systems security (along with regular students). The objective for the gendarmerie is to train these personnel on matters they will encounter in medium to big corporate or public organisations' computer environments

 

Both the university diploma and the master degree diploma have gained from this cooperation in terms of quality and content.

**International Center for Missing and Exploited Children/ Interpol/Microsoft**

The Computer Facilitated Crimes Against Children training seminar was designed to provide law enforcement around the world with the tools and techniques to investigate Internet-related child exploitation cases. This initiative was launched in December 2003 at Interpol Headquarters in Lyon, France. As of November 2008, a total of 3,221 law-enforcement officers from 113 countries have been able to participate in 36 regional training sites in France, Costa Rica, Brazil, South Africa, Croatia, Hong Kong, Romania, Spain, Jordan, Argentina, Russia, New Zealand, Thailand, Turkey, Japan, Norway, China, Bulgaria, Australia, Oman, India, Lithuania, Morocco, Qatar, Panama, Philippines, Poland, Peru, Czech Republic, Greece, Ukraine, Korea, Egypt, Brazil, Colombia and Italy.

The 4-day seminar includes the following modules:

- Computer Facilitated Exploitation of Children
- Conducting the Online Child Abuse Investigation
- Managing the Law Enforcement Response to Computer Facilitation Crimes Against Children
- Prosecuting the Offender
- Technical Aspects of the Investigation
- Resources and Guest Speakers

The financial underwriting sponsor of the training initiative is offered an opportunity to actively participate in this portion of the training. The curriculum is also modified to complement the needs of the host country (i.e., culture, legal, linguistic, law enforcement, etc.).

ICMEC are currently developing an advanced hands on training for technical investigations which is a higher level training where investigators can conduct live investigations.

In addition, ICMEC is now managing the operational role of CETS [3](Child exploitation Tracking System developed by Microsoft) to assist cyber crime investigations. working together with Microsoft on the technical side.

ICMEC is part of the *Financial Coalition* where they are working with the financial services industry to create a mechanism to report cases of illegal transactions such as online purchase of Child Pornography and provide training to Law Enforcement on this mechanism.

[3] Further details on CETS available from ICMEC directly to Law Enforcement personnel

 

**European Union**

The private sector and law enforcement are encouraged to assist each other with education, training and other support on their services and operations.[4]

In 2001 the FALCONE project entitled "*Training: Cybercrime Investigation - building a platform for the future " was launched*. This was a European Commission funded initiative that enabled a group of experts from LE and academia to meet, discuss and agree a set of recommendations for the future shape of Cybercrime Investigation training. The UCD Centre for Cybercrime Investigation became involved as a partner.

This was followed by the AGIS 2003-2006 projects. These projects implemented the recommendations of FALCONE by developing accredited modularised European training programmes for LE. The UCD Centre for Cybercrime Investigation supported these projects through the provision of content experts, academic oversight and accreditation, course trainers, hosting of meetings and development of final report recommendations.

A further FALCONE success was the creation of a Europe-wide working group that would continue to promote and develop harmonised training programmes for Law Enforcement and the Europol Cybercrime Investigation Training Harmonisation Group, formed in 2007, fulfils this role. (UCD CCI has been a member and provided pro bono support since its inception.) The group currently has two major initiatives scheduled for 2009; the upgrade of the existing training programmes, and the 3 year ISEC project under which 30 LE officers will graduate from UCD with a Masters in Forensic Computing and Cybercrime Investigation.

The upgrade project is being jointly managed by staff from the UCD Centre for Cybercrime Investigation and the German Police. UCD has taken responsibility for the financial administration of the project, will host a number of the meetings, and also provide a training designer for all upgrades.

Microsoft has partnered with Interpol, the EU, universities and 15 EU member States to help fund the AGIS Projects which emphasises cooperation among public and private entities in fighting cybercrime. The Project promotes standardised training programs and information networks across participating countries. The AGIS project came to its conclusion, and its successor is ISEC, under the new programme "Prevention of and Fight against Crime as part of the general programme Security and Safeguarding Liberties". Microsoft is working to participate in this new programme.

[4] Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, Brussels, 27-28 November 2008.

 

**Council of Europe**

In order to counter cybercrime and protect computer systems, Governments must provide for:

- effective criminalisation of cyber-offences. Legislation of different countries should be as harmonized as possible to facilitate cooperation
- investigative and prosecutorial procedures and institutional capacities which allow criminal justice agencies to cope with high-tech crime
- conditions facilitating direct cooperation between State institutions, and between State institutions and the private sector
- efficient mutual legal assistance regimes, allowing direct cooperation among multiple countries.

The Convention on Cybercrime (ETS 185) of the CoE helps countries respond to these needs. It was opened for signature in November 2001 and by December 2008 had been ratified by 23 and signed by another 23 countries. The Additional Protocol on the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189) of January 2003 had been ratified by 13 and signed by another 21 States. Equally important is that a large number of countries worldwide is using the convention as a guideline or model law for the strengthening of their cybercrime legislation.

In order to support countries worldwide in the implementation of this treaty, the Council of Europe in 2006 launched the Project on Cybercrime (www.coe.int/cybercrime) which was funded from the budget of the Council of Europe and contributions from Estonia and Microsoft. Phase 2 of this project will start in March 2009 and last until June 2011.

Under this project, the Council of Europe supports training on

- Cybercrime legislation
- International police and judicial cooperation
- Law enforcement – service provider cooperation
- The prosecution and adjudication of cybercrime offences

**Simon Fraser University (SFU) International Cybercrime Research Centre, Canada**

A new research centre to fight cybercrime is being established at SFU's Surrey campus, with a $350,000 grant from the provincial government. The centre is a joint venture of SFU, the province, and the International Society for the Policing of Cyberspace (POLCYB), a British Columbia based non-profit organisation established to prevent and combat crimes on the

 

Internet. The International Cybercrime Research Centre will investigate online crime trends and help to develop new tools to counter cybercrime.

As one of its initial projects the centre plans to develop virus scanner-like tools to detect child exploitation images.

SFU will bring cross-disciplinary expertise in computing science, engineering, and criminology to the new centre, with the statement that "*There is no university in North America I'm aware of with a dedicated cybercrimes studies program*," Huge demand is expected at the graduate and undergraduate levels, as well as professional-studies certificate courses through Continuing Studies.

**United Nations**

Among other organisations preparing cybercrime training initiatives is the UN, through the UN Office on Drugs and Crime that is developing a project entitled "*Establishing and strengthening legal and policy frameworks to address cybercrime in developing countries***".**

The proposed framework, which will target developing countries, is comprehensive and will draw on the expertise and experience of those partners already active in the field. It aims at fighting computer-related crimes in four ways:

- Assist Member States in the adoption of adequate legislation that would constitute a solid basis for effective investigation and prosecution of computer-related crimes.
- Build the operational and technical knowledge of judges, prosecutors and law enforcement officials on issues pertaining to cybercrime.
- Train the judicial profession to effectively use international cooperation mechanisms to combat cybercrime.
- Raise awareness of civil society and create momentum among decision-makers to coalesce efforts to prevent and address cybercrime.

The key aspect for the purposes of this paper is the second objective which reflects the work currently being carried out by a number of the other initiatives. UNODC is a full member of the Europol Working Group on the Harmonisation of Cybercrime Training and will directly benefit from the creation of the proposed Network of Centres of Excellence.

UNODC is also partnering with the Korean Institute of Criminology to develop a virtual cybercrime forum which will provide training and research. Industry is also involved as a partner of this project and provides funding for the infrastructure for the forum.

 

**Industry Initiated**

The French Internet Access and Service Providers Association (AFA) has been involved since 2003 in training sessions about co-operation between ISPs and LEA, organised by the NTEC (specialised investigators in High tech crimes) and the French National School for the Judiciary.

In August 2006, Microsoft has launched a website portal for law enforcement authorities around the world. The Law Enforcement Portal (www.microsoftlawportal.com) is designed to provide law enforcement with easy access to training material and resources related to cybercrime. This portal is a response to the growing volume and variety of requests from law enforcement to Microsoft, related to its software, game or online services. The materials include summaries of various online threats – including children's safety, phishing, spyware, spam, and malicious code – and information about organisations, partnerships, and other resources available to help law enforcement understand, investigate, prevent, and address these threats.

In December 2004, Microsoft announced the Digital PhishNet (DPN), an alliance between law enforcement and industry leaders in a variety of sectors including technology, banking, financial services, and online auctioneering. This alliance is directed specifically at sharing information in real time about phishers to assist with identification, arrest, and prosecution. DPN is the first group of its kind to focus on assisting law enforcement in apprehending and prosecuting those responsible for committing crimes against consumers through phishing.

It provides a neutral, confidential and collaborative forum between the private and public sectors where information about instances and trends of phishing and related cyber-threats can be shared in confidence, analysed, and referred to law enforcement and various anti-phishing services, leading to aggressive enforcement and deterrence of future online offenses. It is managed by National Cyber-Forensics & Training Alliance (NCFTA), a non-profit public/private organisation in the US, with staff from both law enforcement and industry. NCFTA provides training and support for LE; it connects law enforcement with industry experts for analysis and forensics. NCFTA is funded and supported by its members. DPN is organising closed meetings between industry and law enforcement to facilitate cooperation. After Chicago in 2005 and New Orleans in 2006, DPN expanded to Europe with Berlin in June 2007 and to Asia with Singapore in January 2008. It met again in the USA in San Diego, California in September 2008.

Microsoft has developed materials to help law enforcement officials understand the ways in which available technology and software can be used to investigate cybercriminals. These materials include information relating to the technical details of Microsoft's products and

 

guidance for conducting investigations on computers and other devices using Microsoft software.

In October 2006, Microsoft has hosted the “LE Tech 2006” conference at Microsoft headquarters in Redmond, Washington. Gathering around 300 international law enforcement officers from over 45 countries, the event has introduced law enforcement officers from around the world to Microsoft’s newest efforts to assist in cybercrime investigations, including the Child Exploitation Tracking System (CETS), Microsoft’s new Law Enforcement Portal, and Microsoft’s enforcement programs.

In Germany eco organises regularly legal and technical workshops for the abuse teams of ISPs. These seminars are now regularly delivered since they have been considered very useful by the staff participating.

For 2008 eco planned in cooperation with the Federal alliance of the German detectives (Bund deutscher Kriminalbeamter – BDK) a technical and a legal workshop as a road show throughout Germany for the staff of LEA. eco has developed a range of technical and legal materials to help law enforcement officials and detectives better understand the specific internet technical issues and to discuss together the current legal trends and topics.

In January 2008, Microsoft and eBay/PayPal/Skype provided five day training to more than 40 experienced computer related crime investigators from the European Union Member States on malware and botnets. In June 2006, Microsoft organised with Europol a 4 day training course for 24 high tech crime investigators from 15 member countries and in addition 12 people from Europol High Tech Crime Center and other specialised units of Europol. The training covered advanced Windows XP Forensics above and beyond what the available tools cover, MS Office Metadata and Hiding Techniques, Botnet Malware Detection and Analysis, Windows Vista Security Preview and Demo as well as the ICI team's response to the malware threat. Access was granted. Microsoft Windows Vista BETA was also discussed.

With regards to training, Microsoft sponsors or hosts training around the world with regards to a variety of threats, capacity building and child protection. Examples include:

- **The International BotNet Taskforce** (IBTF) started in 2004 and is an annual meeting where international law enforcement, industry partners, security researchers, and private company can come together to discuss ways in which this community can work together to curb the threat of BotNets. This series of conference is seen as one of the premier of its kinds and the participants are of the highest calibre in their respective fields. The 8th IBTF meeting took place on 21st October 2008 in

 

Arlington, Virginia (USA). With representatives from almost 40 countries and close to 200 attendees, this meeting represented one of the broadest selections of attendees in the 4 year history of the conference, combining participants who came for the first time and members that have been involved from the beginning.

- **Law Enforcement Tech 2006 and 2008** (LE Tech): LE Tech was an intensive three-day training designed to equip law enforcement with the latest technology tools and information for cybercrime investigations. The conference focused on technical details and "know-how" around Microsoft's latest products and services.

Through LE Tech and similar trainings, Microsoft has helped train over 6,000 law enforcement officers from over 110 countries (including 1500 in the United-States) around the world and is able to provide the necessary tools and skills to identify cybercriminals.

Initiatives taken by eBay include:

- The Nigerian Economic Financial Crimes Commission
- Training of 60 criminal judges/prosecutors organised by Berlin Senate of Justice.
- A Joint Training Session /conference conducted by eBay, CBI and Interpol for Top 350 LE officials in India.
- The majority of detectives within the UK's Serious and Organised Crime Agency (SOCA) have been trained throughout the year.
- National Magistrates Institute, Bucharest Romania – "Train the trainers" session for 2 groups of judges and prosecutors.
- Europol's High Tech Crime Expert meeting at The Hague. Also a member of the Europol Working Task Force, currently developing training curriculum for '09.
- Trained investigators from all over world at the Digital Phish Network, Berlin – a private/public forum, cosponsored by PayPal.
- Chisinau, Moldova – one week joint training with FBI. As a result, a network of mules moving high value items from Moldova to Romania was stopped
- In 2008, over 2000 Law Enforcement and Trading Standards officers were trained either through organised programs at eBay UK or through outreach at their forces or local offices.

**Other**

There are a number of cybercrime training programmes being conducted by European law enforcement agencies, often through national training centres. These are primarily for law enforcement. In addition there are programmes that allow both law enforcement and industry

 

delegates. Several of these latter offerings are arranged by not for profit organisations such as the High Tech Crime Investigators Association (HTCIA) and the International Association of Criminal Investigators Association (IACIS) which both emanated from the USA and have international chapters. There are well known training programmes that are open to both industry and law enforcement. Perhaps the best known of these is the SANS Institute in the USA.

## 3.2 Current state of cybercrime training and qualifications

Currently available to Industry and LE (including academic and competence based activities)

It is now more common for LE cybercrime training programmes to be associated with academic qualifications. Examples of this are found at The Royal Military College of Shrivenham through Cranfield University (open to non law enforcement), Canterbury Christ Church University, both in the UK and University College Dublin through its Centre for Cybercrime Investigation in Ireland. Other EU countries are also entering partnerships with Universities.

There are also many initiatives in North America and to a lesser extent other parts of the world such as the Asia Pacific Region. The importance of the qualifications that are available through the initiatives mentioned above are that they have all been created through partnerships between academia and law enforcement that ensure the needs of law enforcement are met in terms of students not only being academically qualified but competent to fulfil roles within the law enforcement community.

The last few years have seen many other universities offering forensic computing courses that appear to be computing courses with additional forensics modules that may be acceptable academically but do not provide the knowledge and skills for students to gain employment in the law enforcement environment. Some of this latter group have stated they have created these courses as a direct result of pressure for revenue generation and because the “CSI generation” of students are more likely to enrol than on traditional computer science courses.

This has created two tiers of qualifications and further work is required to identify the “ideal” programme to be followed for students who wish to enter the field of IT Forensics and Cybercrime investigation with the correct level of knowledge and skills to be fit for purpose. This applies equally to law enforcement and industry

There are qualifications available to industry staff although these tend to be more in the areas of information security than IT Forensics and cybercrime investigation. There are many industry personnel involved in cybercrime investigation and it is clear that they need

 

access to the training programmes and qualifications that in some instances are only available law enforcement. Although competency based assessment is a key part of many of the training programmes and some of the qualifications, there are no national or international standards that drive this activity. Many product vendors offer what they claim are certifications which in many instances are not much more than certifying the use of the product. Worryingly many vendors are willing to offer certificates to students based simply on course attendance which adds to the likelihood of incompetent practitioners. Clarity is required in relation to the extent that the study should involve activity outside of Europe given the timescales and resources available.

# 4 Gather information from law enforcement regarding

## 4.1 Currently Available training activities

The IT Forensic and Cybercrime Investigation training activities that are currently available to Law Enforcement fall into a number of categories:

- National and regional training programmes such as those in the UK, Belgium, Germany, Canada, USA and France to name a few
- Invited international guests to the above programmes
- Training workshops held at cybercrime conferences
- Training delivered by international police organisations such as Interpol and Europol
- Industry training initiatives to support law enforcement activity
- Software and hardware vendors
- Training initiatives developed by national governments and/or international organisations
- Training cascaded by those having attended one or more of the above initiatives
- Training available as a result of initiatives such as the EC funded Falcone/Agis/ISEC programmes
- Training on cybercrime legislation by Council of Europe, US Department of Justice, the Organisation of American States and others

Historically, training has been developed in isolation with little collaboration. It was for this reason that the original Falcone cybercrime training programme was created. Many countries and organisations were found to be developing almost identical training modules. This was seen to be a waste of scarce resources and the concept behind the project was to create a framework that would enable training to be developed collaboratively and delivered and made available free of charge to law enforcement on a global basis.

There are currently 7 such courses that have been piloted and made available. These have been translated into a variety of languages, included in national training programmes and delivered in many parts of the world. There is however no coordinating body to ensure quality standards are maintained and that course material is current and where translated, made available to as wider audience as possible. The role of distribution of the materials currently rests with Europol for Europe and Interpol for the rest of the world. There is no campaign to market the availability of the material.

There have been other attempts in the past to attempt to coordinate training activity; such as the International Cybercrime Training Action Group (ICTAG), an initiative of the Canadian

 

Police College and involving cybercrime training centres from a number of English speaking countries. This and similar initiatives were not successful as they had no full time resource devoted to looking after the activities of the group. This is another example of why network coordination is required for any international solution.

It would not benefit this paper to simply list a series of training courses and their content and this has therefore not been done. The training on offer falls into various levels from the first responder through to the most advanced technical training; however it is the duplication of effort and the lack of overall standards that makes it difficult for training undertaken in one jurisdiction to be accepted towards qualifications in another.

It is right to say that the most developed countries, in general have the most advanced training programmes and the opposite is true of the least developed countries. Cybercrime knows no boundaries and it is incumbent on those countries and organisations that have programmes to make them available to those with the greatest need. The most effective way of making this a reality is to create an environment where a structured training programme with appropriate qualifications is available to all.

### 4.2 Currently available qualifications

Various qualifications exist as detailed in Section 3.2 above. The majority of collaborations to create such awards are in English speaking nations. In broad terms the qualifications fall into the categories of IT Forensics and Network or Cybercrime Investigations and the patterns of these qualifications indicate that they are at the correct level across international borders.

### 4.3 Currently available competency based certifications

The majority of competency based certifications in IT Forensics are offered by software vendors and are based very much around their products and services. Many training courses created by vendors have no pass or fail criteria which can therefore promote incompetence rather than competence. Vendors try to mitigate this by offering their own in-house competency based certifications. The problem with this is that the certifications are not compulsory, leaving many hundreds of practitioners who have received a certificate from the vendor for attending a course, but have not undertaken any assessment of their competence.

The International Association of Criminal Investigative Specialists (IACIS) has for a number of years offered competency based assessment certifications. They, however rely on a large number of volunteers to mentor students over a 12 month period which may limit their ability to take on large numbers of students.

 

## 4.4 Details of standards that apply

This section describes the standards that apply to the area of digital forensics and cybercrime investigations and their relationship to points 3.1, 3.2 and 3.3

There are no recognised international standards that apply to either digital forensics or cybercrime investigations. There are however several good practice guides that promote "*principles of computer based evidence*". Two of the longest standing of these are the principles adopted by the Association of Chief Police Officers in the UK in 1998, later adopted and modified for an international audience by the International Organisation on Computer Evidence. These principles of good practice were later adopted by the G8 Countries and have formed the basis of many countries own good practice guidelines. A European Guide was developed with the assistance of funding from the European Commission Oisin programme.

The only standard that has any real relevance to the subject matter is ISO 17025 for forensic laboratories which is currently applied in France and many other countries. For those situations it is an appropriate generic and internationally recognised standard. The forensic IT department of the "*Institut de recherche criminelle de la gendarmerie nationale*" is applying in 2009 for accreditation on that basis. It is not envisaged to apply ISO 17025 to local teams of forensic IT specialists, but the accredited methods and the quality assurance methodology will be progressively introduced, and we welcome the possible development of an adapted accreditation scheme for such teams.

It is important to acknowledge that some of the crimes that are committed using technology and are referred to as Cybercrimes are in fact traditional crimes using a different method. It therefore follows that traditional investigative techniques continue to play a great part in this type of investigation. The international nature of cybercrime brings new challenges and these are typically dealt with by existing international treaties. The one beacon of light is the Council of Europe Cybercrime Convention which seeks to harmonise activities in this area.

## 4.5 The law enforcement requirement for cybercrime/investigation training

The law enforcement requirement for training can be broken down into the following broad areas for specific groups:

- **First Responders:**
  - Preserving the electronic crime scene
  - Legal Issues
  - Identifying, collecting and transporting electronic evidence
  - Asking the right questions of victims, witnesses and suspects in cybercrime investigations

 

- **General Crime Investigators:**
  - As First responders plus:
  - Investigative techniques for online crimes such as identity theft and fraud
  - Conducting online child abuse investigations
- **Network Investigators**
  - As first responder plus:
  - Investigative techniques for network investigations
  - Introduction to Networks and types of crime
  - Advanced training as necessary to fulfil the role
- **Internet Crime Investigator**
  - As first responder plus:
  - Acquiring online information to support investigations
  - Analysing and evaluating online information
  - Function and operation of Internet utilities
  - Tracing individuals through Internet and other resources
- **Covert Internet Investigator**
  - As Internet Crime Investigator plus:
  - Describing the equipment necessary for covert activity
  - Evidence capture and corroboration of covert activity
  - Best practice in legend building and field craft
  - Legal issues and statement making in a covert environment
- **IT Forensics Examiner**
  - As first responder plus:
  - Introduction to computing
  - Introductory IT Forensic Training
  - Specific IT Tool training according to needs
  - Advanced training as required depending on role and required specialism
- **Managers of IT Forensic and Cybercrime Units**
  - As first responders
  - Budgets and forensics equipment requirements
  - International investigations
  - Staff skills set requirements
  - Effective management of investigations involving technology
  - Managing Intelligence led operations

The list is indicative of the differing requirements and further detailed requirements are available. All the above groups require continuing professional development to keep up to

 

date with changes in technology and new forensic and investigation tools and techniques. This section does not seek to address the requirements of others in the criminal justice system such as lawyers and judges.

The objective of training is always to provide key skills in order for students to improve their ability to perform their work functions. Cybercrime training must specifically address:

a- a fast moving technological and legal environment

b- a strong international component (cooperation between states, between LE professionals, LE training organisations international companies; on the other side international cooperation of offenders)

c- credibility of law enforcement professionals in court

## 4.6 Current training delivered to industry

There is little evidence of coordinated delivery of training by law enforcement to industry. There are organisations such as the High Tech Crime Investigators Association (HTCIA) that allow both industry and LE to attend training delivered during their conferences. A similar situation exists in the UK with the First Forensic Forum (F3) that holds an annual conference and one day training events that are open to both groups as is membership of the organisation. There is evidence that many of the on line support fora, while not being a specific training platform, do allow participation from LE and industry members. Many of these such as the High Tech Crime Consortium (HTCC) and Digital Detective, both of which have over 4,000 members allows exchange of information of a technical but non case specific nature.

## 4.7 Current training delivered by industry to law enforcement

Much of the training delivered by industry to Law Enforcement occurs as a result of requests to deliver training from the law enforcement community. It is recognised that this training is normally delivered outside of any structures training programme and to meet specific needs in a location or to provide knowledge to combat certain types of crime. There is no evidence that this training has any measurable lasting effect and no assessment of the suitability of the students is normally undertaken.

Industry spends large sums of money on its law enforcement support programmes and it is clear that this could be better spent by cooperating with organisations that are involved in the delivery of structured training programmes that lead to certification and qualifications. It is not easy for industry to identify these organisations and the proposed collaborative approach to Centres of excellence will give industry focal points with which to work in the future to

 

deliver effective training with lasting results. This will provide a better return on investment for industry and more effective LE investigators.

Industry also participates in delivering training, normally in national LE training programmes to provide a high level of expertise and knowledge to students. These inputs are normally arranged through personal relationships.

## 4.8 What LE knows about the Industry training requirements

Understanding the Industry requirement for training has not been high on the Law Enforcement agenda in the past. Restrictions on the activities of law enforcement often prevent the possibility of joint training or training delivered by LE to industry. National LE cybercrime training centres do receive requests from industry for training and these are very much in line with the training delivered to LE with additional requests for interview skills and investigative skills training. The industry requirement can perhaps easily be identified by the fact that it often recruits LE officials that have the requisite skills, indicating that the need is very similar. It could be said that if LE was more open to training industry there would be less need for this type of "skills poaching" to take place and LE would benefit more from the training it provides its staff. LE contributing to the Centres of Excellence in terms of training provision will be essential to its success.

## 4.9 Target Audience

The key targets of this report in the LEA arena include:-

- Cybercrime Investigators
- Crime investigators with an online element
- Prosecutors
- Forensic Analysts

# 5 Gather information from industry regarding

## 5.1 Current training delivered to LE and the cost where known

Nearly all industry players who have interaction with law enforcement provide ad-hoc training or ad-hoc operational support on request to law enforcement. eBay/PayPal, Google and Microsoft have directly confirmed that they provide a wide variety of training seminars on both software products and services they host and on general Internet technologies. Many of the European ISP associations also provide class-room based training to law enforcement. The costs for these activities are varied since many of the seminars and training session are delivered by local in-country experts where possible or, where that is not possible, the costs are distributed across different cost centres in the organisations concerned. However, in some projects funding commitments for agreed training schedules have exceeded US$500,000.

## 5.2 What industry knows about the LE requirement for this training

The industry assessment of law enforcement requirements are driven in two specific manners:

Firstly, the requirements are identified by industry players from experience gained in the daily operational interactions with national and international law enforcement. Incomplete requests for assistance and inadequately specified requests indicate areas where training can be provided.

Secondly, the requirements are identified in conjunction with law enforcement where day-to-day interactions with law enforcement in the support of ongoing investigations highlight areas where specific in-depth training would be of benefit to law enforcement.

In addition, it is clear that personnel responsible for the day-to-day relationships with LE (those who respond to hundreds of LE requests every week) often have very little training for this role. Sometimes, interim personnel are employed with no specific training. It is important to "professionalise" this activity. For senior ISP personnel, there is sometimes a challenge to understand what the mission of LE is when they will deal with them and what the requirements in terms of evidence preservation and collection

For "fraud" teams or "investigative" teams within the industry, there is limited experience of the LE world and this creates a number of difficulties when it is time to file a complaint, prepare evidence, who to call, etc... Often people try to deal with criminal issues completely "in-house".

 

## 5.3 Currently available qualifications for industry

There is a range of accreditations which are available on a commercial basis from specific product vendors or vendor-independent accreditation e.g. (ISC)[2] CISSP[5]. The working group agreed that these qualifications are often inadequate in the specific area of IT forensics since they are not developed in conjunction with law enforcement requirements. As a result these qualifications tend to emphasise IT, IS and Network security issues and cover post-incident processes and procedures inadequately particularly in relation to evidence collection, tracking or contamination.

## 5.4 The industry requirement for cybercrime/investigation training

Industry of all types is the victim of crime. Any organisation which uses information services and IT networks which are connected to the Internet are exposed to all the risks which internet connectivity brings. Those organisations which consider their I.S. infrastructure as critical to business continuity and competitiveness take steps to protect that infrastructure and the data contained on their networks. This involves internal security audit and ongoing network and systems security monitoring.

When incidents or events are identified which require further in-depth analysis to determine the level of threat or penetration of a system or network attack the security professional requires a high level of knowledge relating to systems and networks security, corporate policies, human resources, legal and regulatory issues and privacy and data protection law. These are in addition to the vast technical knowledge required to analyse and interpret different types of events. Industry require the same level of knowledge as law enforcement personnel in IT forensics. There are some specific areas which might not need to be covered such as undercover investigations except at a general high level in relation to legal and illegal activities. In general, industry responds to incidents on the premise of restoring business activity and services and in mitigating loss to the business and not evidence preservation. Industry would benefit from training in the areas of evidence handling and basic investigative skills to enable them to consider these aspects when dealing with incidents and allowing them to comply with evidence handling best practice to ensure evidence collected will be admissible in court where necessary.

## 5.5 Target Audience

The key targets of this report in the industry arena include:-

- Security IT personnel
- Security IT consultants

[5] (ISC)² is the global leader in educating and certifying information security professionals throughout their careers. Their reputation has earned their certifications numerous awards and global recognition.

 

- Forensic Analysts
- Criminal Compliance personnel

# 6 A vision for the future of cybercrime training

## 6.1 Methods of delivering training

The working group agreed that a centre of excellence should offer a range of levels and methods of training to ensure flexible options are available to match the needs of different categories of students and employers.

The European Commission's Lisbon Strategy for Growth and Jobs identifies 'Lifelong Learning' as a key objective in the drive for Europe's development as a competitive and knowledge based economy.

The needs and requirements of adult learners, most of whom are full-time professionals, are such that learning programmes need to be designed and delivered using a range of methodologies that support flexible modes of learning. This would include classroom delivery, distance, online and blended learning. Development of these programmes within an academic environment will ensure that regardless of the delivery methodology, the content will have been subjected to rigorous academic processes and will meet accepted and agreed criteria.

Learning programmes specifically designed for delivery via a range of teaching strategies will support the European Councils[6] goal of access and inclusion to education for all.

These would include

- Full time: Full time students could participate at a fixed location and dedicate time and attention to a learning programme. This type of programme is most suited to students before they start their career or who are in a position to take a career break in order to change directions in their career.
- Part-time: This type of learning better suits those who are already working and can attend learning at a fixed location for bursts of time (weekends, evenings, two weeks, etc). This type of learning better fits those who are close to the learning institution have a full time career and a personal life which permits them to participate on-site.
- Modular: This type of learning is very supportive to employer and student since it permits bursts of training in dedicated area whereby each module will contain dedicated and focussed learning in targeted areas of direct relevance and providing immediate benefits to both employer and student. It also permits staged learning in bursts of activity and permits learning in any one of the Centres of

[6] http://ec.europa.eu/education/policies/2010/et_2010_en.html

 

excellence throughout a network with credits previously earned recognised throughout the network.

- Blended Learning: Blended learning can be the most effective way to learn and depending on the objective of the blended system can be very flexible to the target student and employer audience or ensure a high level of knowledge and learning by the student.
- Distance Learning: Distance learning is a necessary aspect of modern education and learning. Due to the nature of the modern working environment and the early configuration of the network of Centres of excellence, not all students or employers can be within reasonable distance or access to a centre of excellence. Distance learning provides students with the ability to learn whilst in the working or home environment or to update their skills relating to an updated module which has already been completed.
- E-Learning/ CBT/ WBT: learning using online resources permits the development of a digital training program exactly the way the centre chooses and has the content delivered exactly the same manner every time it is used. Instructors will often change their program to address their needs and tend to vary the delivery of information each time they teach.
- Virtual Classrooms: Combines the best of distance learning with e-learning and enables interactive learning with groups of students who are remote/ distant form each other.
- Podcasts/Webinars: These are extremely useful review resources and to support students who need to apply the topics learnt in their everyday careers. These are a very good method of delivering training for continuing professional development.
- Training Workshops: These normally take place within a conference environment and are also useful for CPD purposes. One downside is that they are often vendor driven.
- Internships:
- Thesis:

## 6.2 Cybercrime Training Centres of Excellence

### 6.2.1 Establishing criteria for centres of excellence at national and international level

The key finding of the study is a requirement for collaboration in the supply of high quality training and education to LE and industry staff. This can best be achieved by creating a network of centres of excellence.

The centres of excellence will develop, on an ongoing basis, the skill set and resources necessary to establish and operate a centre of excellence. The issues which will be discussed by the advisory boards and the centres of excellence will include:

- Centres should be spread across Europe to ensure cultural, geographical and linguistic differences are catered for;
- If possible there should be at least one Training Centre in Eastern Europe or one of the new Member countries;
- Centres should have the appropriate resources (to be defined by the project) to ensure that students are provided with appropriate opportunities to assimilate knowledge and practice skills. This is particularly important with those training programmes which involve formal assessment and, potentially, forms of professional and academic accreditation.
- Centres should have appropriate resources to conduct research into relevant areas relating to cybercrime and to develop solutions to identified issues.
- Centres should have the appropriate administrative infrastructure in place to support their commitment. In practice this means a certain base level requirement in terms of facilities at training centres, their teaching staff and the administrative and tutorial support for students.
- New centres might undergo a form of audit before they are admitted to the network. The audit would examine, inter alia:
  - General ability to deliver services in accordance with the terms of reference;
  - Technical and other facilities available at the Centre;
  - Teaching and training staff suitability;
  - Adherence to security and other professional requirements.
- Centres might also be required to have an academic framework in place to provide qualifications in “Cybercrime Investigations and IT Forensics” and to work with others in the network to allow international students to join programmes.

 

- 2CENTRE will give special attention to develop membership criteria targeted at new centres of excellence in developing economy countries, in order to maximize the global benefit of the project.

### 6.2.2 Network Coordination Centre

The creation of a network of Centres of excellence will require coordination and it is proposed that a network coordination centre be appointed to undertake this role. The network coordination centre would strive to find the right balance between the flexibility required by the networking of the Centre's and the achievement of a concrete knowledge base that could be transferred to new Centres. The network coordinator would seek the close engagement of key trans-national stakeholders in law enforcement (e.g. Council of Europe, Europol, Interpol, OSCE, and UNODC, Asia-Pacific Economic Cooperation (APEC), Association of Southeast Asian Nations (ASEAN), Organization of American States (OAS) and in industry. (E.g. EuroISPA, intellectual property groups, etc)).

The network coordinator would focus on five key areas:

- Encouraging excellence in each Centre.
- Expanding the network to support new Centres and new countries as appropriate
- Supporting external relationships with trans-national agencies and activities
- Promotion of the work of the Centres and the network
- Working with the proposed ISEC project team to further develop the programme

A key role of the network coordinator is to ensure that there are shared and consistent standards throughout the network and that a constant exchange of know-how is taking place on a daily basis among centres of excellence. This will be done by shared mailing lists, restricted members-only areas on a publicly accessible web site and through direct contacts between centres (by email or phone). A more structured way will be established with working-groups focused on specific issues. These issues could be identified by the on-going study comparing the skills and expertise available at the various centres of excellence.

One of the key roles of the network will be the effective exchange of training modules between centres on a bi- and multi-lateral basis. Relationships with centres of excellence outside EU will be established and formalised by both full and associated membership in the network. A further key role is the identification of qualified trainers from both LE and industry to support the delivery of training at national and international level. Currently the international police organisations have no structured approach to managing trainers or

 

providing them with training and technical skills. This could easily be undertaken by the network coordination centre, benefiting LE and international organisations.

Dissemination is an important part of the activity of the network and it will be presented at a wide range of key international events. At the national level, the centres of excellence and the network will be promoted by its national centres of excellence.

The objective of the network coordination centre is to further the co-operation of European centres of excellence which provide training and research to law enforcement and relevant non-law enforcement personnel in cybercrime and IT forensics.. This goal shall be achieved by the network and its members who would seek to improve their co-operation by:

- Furthering the development of best practice papers and codes of conducts regarding the operation of a centre of excellence
- Bundling the expertise of individual centres of excellence for the benefit of the network
- Developing and improving common procedures respecting the national legal and social background of individual centres of excellence
- Setting up procedures and tools for quality control
- Enhancing the network by supporting other initiatives or contacted individuals to establish a centre of excellence
- Increasing the visibility of individual centres of excellence and the network
- Furthering the development of interaction with other relevant initiatives in the area of activity concerned
- Accepting responsibility for maintaining specific training modules for the benefit of the network members
- Leading new projects to develop training modules to benefit the community
- Ensuring visibility by marketing of the facilities and resources that are available and inviting collaborative engagement of appropriate organisations.

### 6.2.3 Industry support for the Centres of Excellence

Promoting better understanding of the work and achievements of centres of excellence is fundamental to enhancing international co-operation with key stakeholders. This includes policymakers at an international level, trans-national governmental organisations, law enforcement, Internet industry and governments among others.

 

Building external strong relationships with many international organisations including Microsoft, eBay, PayPal, Google, Europol, Interpol, United Nations, OSCE and EuroISPA will be essential. A key objective of the work will be to build on and maximise these relationships. In some cases it will be possible to formalise these through putting MoU's in place. Since industry is often a victim of cybercrime it has a lot to gain and contribute to enhancing the knowledge and capabilities of law enforcement in combating cybercrime. Industry can offer knowledge and intelligence on cybercrime trends and provide experts, software, hardware, services, operational support, strategic advice, promotion and awareness raising services and sometimes financial support to ensure a vibrant and successful network of centres of excellence.

## 6.3 Cybercrime Training Advisory Board

### 6.3.1 Advisory board for each centre

This advisory board would counsel the network coordinator and the centres of excellence on issues of concern to the organisations. Their expert advice would ensure that the work of the network and the centres is relevant to the issues faced by cybercrime investigators daily and give more weight and merit to the new ideas and developments brought forward by the centres.

### 6.3.2 Advisory Board skill set

The advisory board would bring together high level representatives of organisations in areas of the world where the centres of excellence are active or plans to be active. These organisations would include international law enforcement agencies, industry and academic representatives, transnational governmental organisations, etc. The work of these organisations must be of relevance to the network and centres.

They will provide guidance and opinions on issues such as:

- New projects and initiatives embarked on by the centres
- Funding and sponsorship
- Promotion at an international level
- Other issues that the centres consider appropriate to be addressed

Advisory board members can be companies or private individuals. However, their work must be of relevance to the centres of excellence or they should be experts on issues that are of concern to the centres of excellence.

 

### 6.3.3 Advisory board for network

An advisory board advising the network would be of significant benefit to the network coordinator and the individual centres of excellence. It would provide an additional level of confidence and ensure transparency and accountability in the network coordination activities.

### 6.3.4 Links with other networks (IMPACT, Interpol, UN, OSCE etc)

The network coordinator should establish and maintain close links with other international or transnational networks active in a similar sphere. The benefits of cooperation among the various players cannot be overestimated and will reduce the duplication of effort currently taking place.

## 6.4 Funding opportunities

It is essential that the 2CENTRE project identifies opportunities for funding of its work. Funding can come in different ways. The most beneficial is direct financial support but donations of hardware, software, tools, training and expertise are also valuable.

IT Forensics and Cybercrime investigation training is expensive and is often dropped in favour of training that allows more people to benefit. This is unfortunate and short sighted on the part of LE management groups. This is further exacerbated by the very small amount of funding available for training in the developing world. These countries are often seduced by vendors into buying unsuitable packages because of a lack of understanding of the correct resource requirements. 2CENTRE must work to improve this situation and use some of the opportunities that follow. Identifying better ways to deliver training will enable the delivery of more events as long as those who currently have training budgets are persuaded of the benefits of the 2CENTRE approach.

Long term sustainability of the network is essential. It is unlikely that national funding of higher education programs will, in most European countries, increase (on a per capita basis): The current economic situation and its long term public debt consequences will not help in this matter. As specific continuing education programs are more and more required to balance their full costs, It will be difficult or even impossible for academia to sponsor LE and industry staff training, in any sustainable fashion.

Nevertheless, there can be considerable benefit to spreading the fixed costs of a programme like this over an open population (LE and industry), as this considerably lowers the cost per capita.

Therefore, operating programs at marginal costs is *possible* when either the size of the program is limited (NTECH) or piggybacks onto non-LE specific programs (Masters Degree).

 

However, It should not be retained as a standard mode of operation when programs grow in size and organizational complexity (specifically, international multi-partner specification of mutualised modules), or upfront development costs (eg. online/electronic resources development).

As an example, the current UTT SSI accredited master's degree program (open to LE and Industry) runs at a full cost of more than €6,600 per year per student (2008 figures including overhead, spread over 26 students over the two years program), and is currently charged a considerably lower sum per capita to Gendarmerie (roughly at marginal costs).

In Ireland UCD course fees are €2,800 per annum for an EU student. However, it is also acknowledged that despite efforts to keep the cost to a minimum, it is still beyond the financial reach for LE officers from many countries (including some from the EU) to undertake the course. LE agencies in many countries simply have no funds to cover such costs for their officers. The provision of a low-cost qualification to support LE is a principle that UCD remains committed to. This principle reflects the University ethos of extending and supporting education provision to the wider community.

In several countries including France, associating with academia makes it is possible to set up foundations that have specific tax status to reduce the cost of financing by industry through tax breaks.

Funding might be sourced from EC Programmes, personally funds, industry, or institutional resources.

### 6.4.1 EC programmes

The development of the successful and continuing Cybercrime Training programme in Europe that has led to the creation of the Europol Working Group on the Harmonisation of Cybercrime Training has benefited from funding from the European Commission Falcone and Agis programmes and the five year plan includes proposals to make further bids to enhance the project. This is a key source of funding and the proposed 2CENTRE project falls within the broad plans already identified for the future. Cybercrime training is once again a priority for the EC ISEC work plan for 2009 and the enhanced relationship between LE, Industry and Academia as reflected in this report should encourage further funding bids as we move forward.

### 6.4.2 Personally funded

There is evidence that a substantial number of IT forensic analysts and cybercrime investigators in LE are paying for training from their personal funds as their organisations are refusing them the training they need to conduct their work with credibility. This is even more prevalent where individuals are seeking to join academic programmes. There is, of course, a

 

case for saying that this shows a commitment on the part of the individual and this will undoubtedly continue in the future, regardless of the propriety of employers forcing this course of action on individuals.

### 6.4.3 Industry Support

Industry has already provided considerable support to LE training and it is expected that this will continue, although the focus will have to be more structured in the future, if the industry objectives for their involvement are to be achieved. The 2CENTRE proposal will provide the capability for this to be achieved.

The opportunities that may be developed as a result of the project for joint training initiatives will offer another route for industry support. The concept or differential pricing for training events is well established in North America where industry participants are charged a premium for training and this in turn allows LE delegates to receive training for a reduced or no cost.

Industry may play a key part in the provision of scholarships to students, particularly from developing countries. These may be used to "kick start" an effective capacity building exercise in these countries in conjunction with the international bodies.

### 6.4.4 Institutional Support

The national organisations may have a training budget which can be used to send personnel to be trained at the most appropriate Centre of excellence. For example, since its official forming in 2006, the UCD Centre for Cybercrime Investigation is actively seeking research funding from national and European funding agencies and from industrial associations. To date the Centre has secured over €1M of research funding from various agencies including Higher Educational Authority of Ireland, Science Foundation Ireland, Enterprise Ireland and the Irish Banking Federation.

In addition, there are opportunities for international organisations to benefit and contribute to the network of Centres of excellence. Those such as UNODC and OSCE to name but two have their own aspirations to deliver cybercrime training to international audiences and particularly those in the developing world

### 6.4.5 Standards and good practice

The lack of standards in the area of IT Forensics and Cybercrime Investigation has led to a myriad of solutions being developed at national and international level. There are good practice guides and these have a level of consistency that demonstrates that the *documented* practice is fairly evenly adopted. This however is not enough, it is necessary for standards to be developed and the creation of 2CENTRE can only assist

 

that process through its harmonisation of training and education. This should be a key task of the new network.

It is believed that accreditation and qualification are complementary processes serving the global purpose of cybercrime investigation.

## 6.5 Research and Development

A further key area which is an integral part of the network of Centres of Excellence is Research & Development, where networking research teams fostering joint research programs and the exchange of young researchers will develop a coordinated approach (with each centre specialising in a domain that is consistent and complimentary within the network) and develop European forensic tools, including open source.

For example, at present, the UCD Centre is conducting a wide range of research projects including but not limited to the following.

- development of automated reconstruction techniques for determining events occurred during cybercrime;
- development of ontology based approaches to cybercrime investigation;
- investigation of application of data mining techniques for network intrusion detection;
- identification of key factors in the prevention and investigation of online financial crimes using machine learning techniques;
- development of generic mobile phone forensics investigation framework;
- investigation of forensic challenges posed by grid computing and related paradigms;

In addition to largely theoretical research the UCD Centre is conducting highly applied research for international police organisations and individual police forces. This includes projects such as

- development of forensic techniques for analysis of Voice over IP communications;
- reverse engineering of malware;
- experimental analysis of illegal distribution of software and other prohibited material on peer-to-peer networks;

## 6.6 International qualifications

Accreditation' is the process by which a program of education/training is recognized as having academic value by the (national) education system.

There are some basic ground rules that should apply where academic accreditation was desirable:

 

- Accreditation is often expressed as credits related to completion of the learning outcomes of a programme. These learning outcomes are assessed in some formal and coherent manner. Hence any academic accreditation is likely to involve a need for robust and verifiable assessment of individual student work;
- Credits should be expressed using the European Credit Transfer System (ECTS) as well as in the host nation's own credit framework;
- Credit should be awarded through the Accreditation of Prior (Experiential) Learning to existing Cybercrime Investigators;
- The accreditation of the training should also subscribe to the principles outlined through the Bologna process now widely adopted throughout 27 European states. It involves compliance to European quality standards, including the European Credit Transfer System (ECTS), and the LMD framework, providing :
    - a formal evaluation/accreditation process
    - assessment of learning outcomes in a formal and coherent manner
    - awarding of modular, academic credit, capitalized towards an academic award such as the Bachelor's or Master's degree (the LMD system) ,
    - transferability to other European institutions.
      (see http://www.bologna-berlin2003.de/en/glossary/index.htm).

There is a difference between 'accreditation' and 'qualification' although in some cases (typically higher education programmes in medical education and training) the two are intimately linked. 'Accreditation' normally involves the awarding of academic credit, often towards an award such as the Bachelor's or Master's degree. 'Qualification' normally involves some form of confirmation of 'fitness to practice'. In the context of Cybercrime Investigation it is important that the 'qualification' has pan-European and global currency and credibility. It follows therefore that an organisation such as 2CENTRE could lead in the establishment of a Register of practitioners.

The experiences of some universities with cybercrime awards suggest that when entering into the accreditation process the following points should be considered:

- Academic credit is only awarded to students who have suitable qualifications or undergo some form of assessment based on experiential learning or formal assessment.
- A related and relevant modular approach to certification.
- The Higher Education Institute approach should be approved by the host nation academic official process e.g. the Higher Education Awards Council (Hetac) in Ireland

 

and the Department for Education and Science (DFES) in the UK. In France evaluation of research and education programs and institutions is provided by the independent agency AERES (Agence Nationale d'Evaluation de la Recherche et de l'Enseignement Supérieur) and accredition is conferred by the French Ministère de l'Enseignement Supérieur et de la Recherche.

- Most educational systems recognize Accreditation of Prior (Experiential) Learning; this will be useful to the integration of existing Cybercrime Investigators; (e.g. Validation des Acquis Professionnels in France, already practiced by UTT for some gendarmes at the master degree level). Such Academic credit is only awarded to students who have suitable qualifications or undergo some form of assessment based on experiential learning or formal
- Both the course and ongoing support given by the Higher Education Institute and the form of continuity available in order to complete their programme, need to be taken in account.

In short, accreditation of programs guarantees the three key objectives : state of the art, international recognition, and credibility in court.

However, it is important to recognise that not all countries require academic accreditation of training and therefore such accreditation of training courses should be entirely optional, at least in the first stages of progress. There are a number of pragmatic reasons for this, not least of which were the very different systems of awarding academic credit throughout Europe and the different systems of police education and training. The national systems of awarding academic credit throughout broader Europe are still in the process of harmonizing.

Both the course and ongoing support given by the Higher Education Institute and the form of continuity available in order to complete their programme needs to be taken in account.

## 6.7 **Accreditation Benefits**

Accreditation may provide the following benefits to LE agencies and personnel:

- Attractiveness to young graduates, who are familiar with and value academic degrees, and to in-the-job professionals; both populations being concerned about the "external" value and recognition of their training
- strengthening of cases in court when facing potentially impressively-educated specialists & lawyers testifying on the other side
- compliance to international standards of quality in education, including
    - Formal evaluation of student work

 

- Evaluation of program elements by students
- Progressive capitalization of learning units
- Capacity of transferring credit at the international level
- Assurance that training at the M (5-year, master degree) level, is rooted in knowledge of the state of the art, provided by faculty with an externally-recognized track record (publications, agency & industry contracts, patents…)
- possibility of partial funding through public funding of education (depending on the country).

## 6.8 Universal recognition

It is important that any 'qualification' has pan-European and global currency and credibility. It follows therefore that an organisation such as 2CENTRE could lead in the establishment of a Register of Practitioners. Admission to the register would be based on qualification and/or academic track.

As the network expands beyond Europe it will be important to establish mechanisms to enable transfer of credit and universal recognition of training and qualifications. Current systems in place for other subjects should assist this process.

The system should be flexible enough to fulfil the needs of LE agencies of most countries, depending on their experience, availability of trainers, training centres, academia, accredited programs, and training capacity (trainers and funding).

2Centre will play a key role in the management of these processes and the "recruitment" of new partners as well as ensuring the standards of the network are maintained by working with its advisory board and the individual Centres.

## 6.9 Qualification/vocational certification

'Qualification' normally involves some form of confirmation of 'fitness to practice'. Its evaluation and recognition is usually conferred by the community of professionals (or organisations) practicing the relevant skills, and does not necessarily involve academic institutions.

In some cases (typically higher education programmes in medical education and training, and/or professions to which access is controlled by a national register) the two are intimately linked.

In other cases, qualification/certification can be capitalized into heavier accredited degree-granting programs, therefore contributing to Accreditation of Prior (Experiential) Learning.

 

Qualification without accreditation could also be useful to LE agencies,

- for basic training programmes (below the bachelor L3 level), possibly evolve into accredited programs
- for short, highly technical programs (e.g. “Vista forensics”)
- for access to non-LE related skills, provided by civilian private or public training centres (e.g. English, or “Elementary Spreadsheet programming”)
- in the case of national training efforts with limited means or limited access to accredited programs and academic institutions.

Note: The European Community has launched an initiative geared at providing vocational/qualification programs the same level of capitalization/international recognition and transfer potential as the ECTS system provides for education. This system, still in development is called ECVETS (European Credits. system for Vocational Education and Training).

# 7 Conclusions

- There is clear evidence that many efforts are being made to deliver “cybercrime” training to Law Enforcement by themselves as well as industry.
- Much of the training currently delivered is uncoordinated and has very little long term benefit.
- Some initiatives such as the EC funded “Cybercrime Training” projects have been very successful, trained many international LE officials and led to the development of academic qualifications.
- There is still much duplication of effort in developing training courses and this is somewhat influenced by the lack of national and international standards in IT Forensics and Cybercrime Investigation.
- Industry has unmet requirements for training in these subjects that mirrors to a great extend those of law enforcement,
- Academic awards in the areas of IT Forensics and Cybercrime Investigation now exist that have been developed with Law Enforcement cooperation to ensure that students are not only academically qualified but are also fit for purpose in the workplace.
- A second tier of qualifications is emerging that are Computer Science programmes with minimal forensic input that do not have the same status.
- Successful capacity building requires a coordinated effort between the above players in an environment where organisational bureaucracy is not an obstacle to the delivery of effective training and education programmes internationally.
- In times of economic downturn, it is essential that all players consider more effective use of resources in order to provide coordinated training that is sustainable and may lead to qualifications and certification and a better return on investment.

# 8 Recommendations

- Countries should be encouraged to create Centres of Excellence in IT Forensics and Cybercrime Investigation to provide sustainable, scalable, standards based and measurable learning opportunities to law enforcement and relevant industry personnel.
- Centres of Excellence should consist of Law Enforcement, Industry and Academia in each country. Each Centre should be physically located in a learning organisation in each country.
- A bid for funding should be submitted in 2009 under the EC ISEC programme to create a Network of Centres of Excellence. The Université de Technologie de Troyes in France and University College Dublin in Ireland should be the lead organisations for the bid working with an independent neutral Network Coordination Centre
- A Network Coordination Centre (2CENTRE) should be created and consist of representatives from Law Enforcement, Industry and Academia. A bid should be submitted to fund this activity during the project period
- Centres of Excellence in training research and education should be encouraged to aspire to membership of the Network and other Centres should be allowed to join the Network during the project.
- The project should work closely with the Europol Working Group on the harmonisation of cybercrime training and Interpol to ensure that their work is provided with appropriate support and the outcomes of the previous EC funded projects are incorporated within the plans for the network of centres of excellence as it develops.
- International organisations should be encouraged to participate in and benefit from the creation of the Network
- The long term aim is to create a sustainable network that will expand beyond European borders and seek to provide a training, research and education resource for Law Enforcement and Industry personnel tasked with combating cybercrime.

# Appendix A- Project partners

## A.1 Law Enforcement

### An Garda Siochana, Ireland

An Garda Siochana is the National Police Service for the Republic of Ireland. The CCIU is the National Computer Crime Investigation Service responsible for the investigation of computer crime, the forensic retrieval of digital evidence. The CCIU have developed a partnership with UCD since 1997 in the development of forensic computing and cybercrime investigation training for AGS and for other LE agencies within the Republic of Ireland. The CCIU currently hold the chairmanship of the Europol Cybercrime Investigation Training Harmonisation Group. AGS through CCIU have been lead partners within the FALCONE, AGIS EU Commission funded projects in the development of an accredited programme of education for law enforcement in Europe. AGS through CCIU are the lead bidders and project managers in another EU Commission Project under the ISEC programme for the final stage of the development of a Masters Degree in Forensic Computing and Cybercrime Investigation for law enforcement in Europe.

### Gendarmerie Nationale, France

The Gendarmerie nationale is one of the two national police forces in France, in charge of public security outside of large cities (50 percent of the French population). Starting in 1998, the gendarmerie nationale has developed a training initiative to cover the needs of the fight against cybercrime and the abuse of digital technologies by criminals in general. Over 200 specialised investigators (called NTECH, 24 new students every year) have been trained and their training is sanctioned since 2005 by a university diploma delivered by the University de Technologie de Troyes.Training partnerships are also being developed with the other national police force (the Police nationale).

## A.2 Academic

### University College Dublin, Centre for Cybercrime Investigation, Ireland

Established in 1881 University College Dublin is the largest university in Ireland with 22,000 students consisting of 16,000 Undergraduates 6000 postgraduates, including 1300 doctoral students. It has 5 Colleges, 35 Schools, and 5 Graduate Schools which employ 2,500 academic staff. 11% of the student population (2,400) are international students.
For over 150 years, UCD has produced graduates of remarkable distinction, including five of Ireland's Taoisigh (Prime Ministers). Perhaps the best known of all its graduates is the writer James Joyce, who completed his Bachelor of Arts at the university in 1902.

 

Each of the five colleges at the university has its own dedicated graduate school with the explicit task of enhancing doctoral and post-doctoral training to match the national strategy of establishing Ireland as a premier source of 4th level education and research.
The School of Computer Science is a recognised international centre for research in a number of key areas including intelligent systems and distributed systems/ubiquitous computing. It has a comprehensive teaching portfolio covering a wide variety of taught undergraduate and graduate programmes combined with a strong innovation and entrepreneurial culture. This culture has been enhanced by the development of strong links with related industry stakeholders.

**Université de Technologie de Troyes, France (UTT)**

UTT is a fast growing higher education, research and contract-work public institute (2500 students, 300 employees). UTT delivers 40 nationally accredited doctorates and 500 M-level (master's degrees and 5 year engineer degrees) a year. A partner of Gendarmerie Nationale since 2001, UTT delivers 45 L-level university degrees and 10 Masters's degrees to Gendarmes every year. UTT's research (100+ faculty active in research) ranges from nanotech to public security, and focuses its development efforts on global security and risk control; UTT is the lead partner of a research network of excellence called 3SGS for "Surveillance, Sûreté et Sécurité, des Grands Systèmes" including academia and industry.

 

# Appendix B - Authors

## B.1 Cormac Callanan

Cormac Callanan operates an independent consultancy company from Dublin, Ireland named Aconite Internet Solutions (www.aconite.com) which provides expertise in policy development in the speciality area of international cybercrime and Internet security & safety. Qualified in Computer Science he has over 20 years working experience on international computer networks and 10 years experience in the policy area of illegal content and cybercrime activities on the Internet. He has provided training at Interpol and Europol and to law enforcement agencies around the world on the subject of emerging and developing technologies. Having visited over 45 countries for business, he currently provides consultancy services around the world and works on policy development with the Council of Europe. In 2008, in conjunction with co-author Marco Gercke, he completed a study of best practice guidelines for the cooperation between service providers and law enforcement against cybercrime (www.coe.int/cybercrime) adopted at the 2008 Octopus Conference.

Cormac Callanan was past-president and CEO of INHOPE – the International Association of Internet Hotlines (www.inhope.org). During this time the network grew to 30 member hotlines in 27 countries around the world and he successfully achieved financial support of over €3m during this time. INHOPE facilitates and co-ordinates the work of Internet hotlines responding to illegal use and content on the Internet. He co-authored the INHOPE first Global Internet Trend report in 2007 which was a landmark publication for policy makers, governments and Industry on Internet child pornography.

Cormac was founding Chairman of the Internet Service Provider Association of Ireland (www.ispai.ie) in 1997 which he led for 5 years until February 2003 and served as Secretary General of the European Service Provider Association (www.euroispa.org). He was founding Director of the Irish www.hotline.ie service in 1998 responding to reports about illegal child pornography and hate speech on the Internet. In addition to representing INHOPE, he has represented the Irish and European Internet Service Provider's at Irish government and at EU level.

Following work on international assignment in the USA and Japan, he established the first commercial Internet Services Provider business in Ireland in 1991 - EUnet Ireland – which was sold in 1996. Cormac is a board member of the Copyright Association of Ireland (www.cai.ie). He served on the Rightswatch (www.rightswatch.com) UK & Ireland Working Group developing best practice guidelines for Notice and Takedown procedures as they relate to Intellectual Property Rights (IPR).

 

## B.2 Nigel Jones

Nigel Jones is currently director of a company specialising in technology risk solutions and training and has recently taken up an adjunct professorial position at University College Dublin. He was most recently European Practice Leader and Managing Director of the Financial and Litigation Consulting Services Practice of a major insurance broker. Prior to this he was responsible for the creation of the National High Tech Crime Training Centre at the National Centre for Policing Excellence at Wyboston in the UK and was responsible for the creation of the design and delivery of a core curriculum and modular high tech crime training programme for the UK police service.

In a police career of 30 years he gained wide ranging experience in major commercial fraud and computer crime investigation. He was the Secretary of the Association of Chief Police Officers Computer Crime Working Group and the UK Internet Crime Forum as well as being the UK Police representative on the G8 sub group on high tech crime and UK coordinator of a series of G8 Industry conferences. During his time as a fraud investigator he designed and delivered an academically accredited fraud training programme.

Nigel formed the Kent Police Computer Crime Unit in 1993 and is co-author of the ACPO "Computer Based Evidence - Good Practice Guide" and member of the Technical Working Group on the Investigation of Electronic Evidence (TWGIEE) in the USA. Nigel has given presentations at numerous national and international events including the preparation and moderation of a hi-tech crime scenario at the United Nations 10$^{th}$ Crime Congress. In 2002 he was appointed by the UK as a member of the Interpol European Working Party on IT Crime.

In 2003 Nigel was appointed as project manager of a European Commission Agis funded programme to develop a cybercrime training programme for the 28 EU and candidate countries. A network of cybercrime training institutes was created to take this work forward. The project was supported by 19 partner organisations within the EU. Nigel was also project manager for a series of training courses course on behalf of the European Police College (CEPOL) to deliver training to senior managers of EU police forces and a further project to deliver training to a group of countries from North Africa, the Middle East and Southern Europe.

In January 2005 Nigel was elected by the Member Countries as Chair of the Interpol European Working Party on IT Crime. and has recently been appointed to the Board of Directors of the Institute of Computer Forensic Professionals,

 

Nigel worked in close collaboration for two years with Canterbury Christchurch University in the development of an M.Sc. award in Cybercrime Forensics that is now offered by the University.

He was recently invited to Interpol as an expert to provide advice on an international IT forensics investigation. He also chaired the cybercrime panel at the recent Interpol General Assembly. He is currently a member of the Home Office Forensic Regulators digital forensics specialist group which is assisting in identifying requirements for new or improved quality standards, applying to the provision of digital forensics services to the police service and the wider Criminal Justice System. Most recently Nigel has been advising Interpol in relation to their international cybercrime training programme and acted as course manager and a trainer on these courses. Nigel and his co-director have also delivered cybercrime training to staff of the Interpol General Secretariat in Lyon as well as the anti-piracy industry in the UK.

**Professional affiliations:**

- Member of the editorial board of the International Journal of Digital Forensics and Investigation.
- Member of the NIJ technical working group developing recommendations for curricula for Computer Forensic programs in the USA.
- Member of the working group developing National Occupational Standards and Core Competencies in the area of digital evidence in the UK.
- Member of the steering committee for the development of a virtual Cybercrime forum under the auspices of the Korean Institute of Criminal Justice Policy and the UNODC.
- Special Advisor to the Europol working group on Cybercrime training.

Nigel was honoured with the award of an MBE for outstanding public service by Her Majesty Queen Elizabeth II in the 2004 New Years Honours List.

 

## Appendix B – Comments Received

| Name | Version | Communication | Date/Time |
|---|---|---|---|
| G. Galarza | 0.8 | email | Fri 20/02/2009 19:49 |
| R. Jansky | 0.8 | email | Wed 18/02/2009 16:30 |
| L-J Brossolet | 0.8 | email | Sun 15/02/2009 15:54 |
| R. Boscovich | 0.8 | email | Fri 13/02/2009 17:54 |
| A. Seger | 0.8 | email | Fri 13/02/2009 12:06 |
| J-C Le Toquin | 0.8 | email | Fri 13/02/2009 08:48 |
| E. Gonzalez | 0.8 | email | Thu 12/02/2009 13:27 |
| L-J Brossolet | 0.8 | email | Thu 12/02/2009 10:37 |
| L-J Brossolet | 0.8 | email | Thu 12/02/2009 10:03 |
| E. Freyssinet | 0.8 | email | Wed 11/02/2009 19:26 |
| J-C Le Toquin | 0.6 | Email | Thu 29/01/2009 15:27 |