

Tilley Award 2005

Application form

The following form must be completed in full. Failure to do so will result in disqualification from the competition.

Please send completed application forms to Tricia Perkins at patricia.perkins@homeoffice.gsi.gov.uk

All entries must be received by noon on the 29 April 2005. Entries received after that date will not be accepted under any circumstances. Any queries on the application process should be directed to Tricia Perkins on 0207 035 0262.

1. Details of application

Title of the project: E-CRIME WALES

Name of force/agency/CDRP: NORTH WALES POLICE

Name of one contact person with position/rank (this should be one of the authors):

CHRISTOPHER CORCORAN, DETECTIVE SUPERINTENDENT, NORTH WALES POLICE

Email address: chris.corcoran@nthwales.pnn.police.uk

Full postal address: NORTH WALES POLICE, CRIME SERVICES DIVISION,
POLICE HEADQUARTERS, GLAN Y DON, COLWYN BAY, LL29 8AW

Telephone number: 01492 511988

Fax number: 01492 511804

Name of endorsing senior representatives(s)

DETECTIVE CHIEF SUPERINTENDENT DUFFIELD, CRIME SERVICES DIVISION, NORTH WALES POLICE

DEPUTY CHIEF CONSTABLE WOLFENDALE, NORTH WALES POLICE

Position and rank of endorsing senior representatives(s)

DEPUTY CHIEF CONSTABLE, NORTH WALES POLICE

Full address of endorsing senior representatives(s)

NORTH WALES POLICE, POLICE HEADQUARTERS, GLAN Y DON, COLWYN BAY, LL29 8AW

2. Summary of application

In no more than 400 words please use this space to describe your project. Include details of the problem that was addressed a description of the initiative, the main intervention principles and what they were designed to achieve, the main outcomes of project particularly in relation to the problem, evidence was used in designing the programme and how the project is evaluated.

E-Crime Wales is a unique partnership initiative between the Welsh Assembly Government, the four Welsh Police Forces, the Welsh Development Agency, Morgan-Cole Solicitors and the National Hi-Tech Crime Unit.

The first ever E-Crime Summit (outside London) was held in Cardiff on Tuesday 8th February 2005 and was attended by 200 delegates; 48% from the private sector, 42% from the public sector organisations and 10% from police forces across Wales.

The purpose of the Summit was to address the threat of e-crime in Wales which currently costs business in Wales in excess of £160 million per year. The recommendations of the Summit have formed the basis of a 'Manifesto' for Wales outlining the priority areas, the partnerships required and the interventions needed to tackle the e-crime problem in Wales.

The agenda for and the four main themes addressed by the summit resulted from discussions which took place at a series of workshops held across Wales in November and December 2004 set up to discuss e-crime, the issues and the way in which it could be prevented.

The four main themes were:

Education and Awareness Raising

(Initially aimed at Small and Medium enterprises (SME's) of the business sector but with a view to setting medium and long term objectives across the education agenda).

Common Practices and Standards

(Dealing with immediate crime prevention and security concerns, but working with business to achieve longer term goals).

E-Crime Reporting, Recording and Visibility

(Under-reporting, lack of statistical information and therefore lack of evidence to support crime pattern analysis and failure to recognise that a crime has been committed and consequences of that e-attack to business and the Welsh economy).

Resources

(Small businesses inability to have in place security and enforcement policies, threat/risk assessments or support and advice to reduce/combat e-crime within their business communities).

Over 400 ideas and suggestions were put forward during the summit, all of which have been taken into account when driving this initiative forward.

The ACPO Strategy for the Investigation of Computer Enabled Crime (Jan 2005) states that "The convenience and advantages brought by the internet and information technology have also created new opportunities for criminals. There is no doubt that hi-tech crime will be increasingly represented in the yearly volume of criminal offences".

As a result of this initiative Wales is now at the forefront of a multi-agency response to tackle e-crime through reduction, prevention and detection strategies supported by the Welsh Assembly Government and the private and public sector communities within the region.

3. Description of project

Describe the project following the guidance above in no more than 4000 words

In 2003 following numerous publications and NOP World surveys (United Business Media 2003) it became very apparent to the Police forces in Wales that much was being said but little done in a proactive manner to stem the flow of information and communication technology-related crime and abuse both to the public and private sectors of our communities.

It soon became obvious following basic research that as computers have become increasingly widespread in modern society, so their use in criminal activity has increased.

Hi-tech crime, like domestic violence, happens behind closed doors and we soon realised that victims in industry playing host to abusers would not solve the problem on their own. Partnerships are not just about working with victims, they are about working to prevent victimisation.

In order to tackle and to take a crime preventative stance on this ever growing threat of e-crime in Wales, we set up our very own e-crime partnership between the four Welsh police forces, the Welsh Assembly Government, the Welsh Development Agency, Morgan Cole Solicitors and the National Hi-tech Crime Unit with our mission statement as:

- To combat serious and organised hi-tech crime, making Wales a safe place to live and work
- To advise and inform on current risk and solutions
- To develop these solutions, through close partnership between business, law enforcement and government in Wales.

The Police Service in Wales is divided into separate Police Force areas. North Wales / Dyfed Powys / Gwent and South Wales.

The Welsh Development Agency has it's Headquarters in Cardiff and a number of satellite offices across Wales.

The specialists within each of the Force Hi Tech Crime Units act as a single point of contact to support business in their concerns about Hi Tech Crime and other emerging trends in criminal use of technology. However, with 150,000 small and medium enterprises (including sole traders) the limited resources are unable accommodate all requests but can offer guidance and onward referrals to other specialist companies.

Details of the Problem and Description of the Initiative

In 2004 84% of businesses in the UK claim to have suffered from at least one computer related incident or e-crime in the preceding 12 months. E-crime ranged from spam e-mail, virus infection, theft of computer/lap tops, credit card fraud, hacking and identity theft, all with financial loss to companies (National Hi Tech Crime Survey 2005). Indeed statistics from the National Crime Squad and National Hi-Tech Crime Unit indicate that £2.4 billion was lost in the UK to e-crime in 2004 and 9 out of 10 companies now suffer from e-crime in the UK.

Within Wales it is estimated that at least £160 million is lost to business through e-crime each year (Source – Welsh Development Agency 2005).

The willingness and enthusiasm to stem and prevent this massive drain on the business economy and communities in Wales was taken up by the multi-agency steering group, who from the outset were determined to take the fight back to source.

Following a decision to hold an e-crime summit for Wales, the first ever such project for any UK region (outside of the National Hi Tech Crime Congress, London) all small and medium enterprises in Wales (SME's) were invited to forward their e-crime concerns which could be addressed at the summit both by peers and experts in the field.

From the responses returned by the private and public sectors and law enforcement, it was overwhelmingly apparent that no one had any concept as to the real problems, or even in some cases basic awareness of how e- crime was affecting their own transactions, and day to day dealing with other industrial partners both within the UK and abroad.

Utilising messages, such as 'Setting Business Free from Crime' (Crime Survey - British Chamber of Commerce 2004) the steering group reinforced the message of 'given the importance of information and communications technology (ICT) computer related crime and e-crime in particular has the potential to cause immense problems for firms that fall victim to incidents of this nature'. In order to avoid the potentially devastating consequences of this type of crime it is essential that companies take measures to prevent such incidents, by building security into their business systems.

Businesses throughout Wales have acknowledged this message but have no processes or expertise in which to progress security issues.

When posing the question, 'Is there really a problem?' most respondents stated that there was one, even amongst the public in general especially home based users of the internet, there was a very real feeling of vulnerability. The simple truth is that we don't know for certain what the extent of the risks are for users in Wales at the present time, but there is a very high risk indeed that we in the law enforcement and business communities seriously underestimated the threat from and impact of e-crime.

How can we know the scale of the problem if we do not properly report and record it. If we do not know the scale of the problem (UK wide, not just Wales) then how can we ever induce or initiate an appropriate police response or ensure adequate resources and crime prevention initiatives.

Intervention Principles

Due to the identified gap in knowledge expressed by the business communities and a plea from the public sector for assistance to make systems more secure, the multi-agency steering group realising that the lack of preparedness by business could result in just one single e-crime attack or denial of service, potentially putting SME's out of business.

To address this initial problem and in order to evaluate the true scale of the problems currently encountered by both the private and public sectors in their daily functioning, the group held a series of four workshops across the whole of Wales during November and December 2004.

The workshops provided an opportunity for stakeholders, including the police and other law enforcement professionals, the public sector and industry to discuss e-crime and begin to explore ways in which this type of crime could be prevented in Wales.

The workshops identified the key challenges to businesses and consumers seeking to adopt secure on-line practices, such as:

- Lack of awareness and education
- Lack of visibility of e-crime
- SME's lack of resources
- Staff as a security threat and lack of security expertise
- Lack of security policies and enforcement
- Lack of support and advice
- Unavailability of insurance
- Lack of common risk assessment standards and methodologies
- Failure to understand the risks of broadband

The workshops further provided the opportunity for stakeholders to be open and frank in a confidential environment in regard to specific concerns and security issues pertinent to their respective areas of business.

A consensus view from all workshop delegates was that there was an absolute need for a continued multi-agency partnership approach to addressing the e-crime threat, not just the existing partnerships but the need for a wider group as appropriate, of committed stakeholders and other Welsh based organisations such as for example, the Federation of Small Businesses.

Some of the potential solutions as discussed by facilitators and stakeholders included:

- Raising awareness
- Education
- Making IT a boardroom issue
- Developing common security guidelines appropriate for Welsh businesses
- Providing a central point of advice
- Identifying groups which can assist in the prevention of e-crime
- Better use of technologies
- Availability of insurance

With 68% of small and medium enterprises (Ofcom, 2004) in the UK now connected to the internet and with unprecedented global access to both information and individuals, the Internet represents a major societal force in areas as diverse as education, commerce, community formation and a whole host of opportunities. Unfortunately it is equally amenable to misuse.

Computer or Hi Tech Crime, is becoming an increasing concern to a variety of regulatory and law enforcement sectors. The information technology age in which we live means the scope for information technology-based crime and abuse is extensive and diverse. Those with a role to play in its reduction form an equally diverse community. All of these agencies and bodies need to work in a timely and co-ordinated manner in a rapidly changing environment.

The multi-agency, steering group set out to achieve close working relationships in this challenging, but necessary mission in order to place the potential solutions as identified by stakeholders into a real programme for action.

OUTCOMES

Under reporting of e-crime was identified as a real problem. If we do not know the true scale of crimes committed in Wales then we cannot ensure adequate allocation of resources or an appropriate policy to deal with it.

Therefore we have now moved towards a three pronged approach to address the problem.

- (i) Adequate intelligence gathering in line with the National Intelligence Model (NIM) in order to direct appropriate resources and responses to emerging threats
- (ii) Maximising the use of the National Hi-Tech Crime Unit (HTCU) Confidentiality Charter which is designed to help business understand how it can interact with local Hi Tech Crime Units in a secure, efficient and confidential manner, whether by passing information for intelligence purposes only or by reporting hi-tech crime for investigative purposes.
- (iii) Utilising the University of Wales in conducting a research and analysis project to examine the way in which the Police Service in Wales receives and records e-crime (using North Wales Police as the point of contact).

By increasing and improving our intelligence capabilities we can increase the risk to offenders to more detections, disruption and arrests.

Awareness raising and education plays a major role in both crime prevention and intelligence gathering. Prevention is better than cure, a key message taken from the workshops and the summit itself. We recognise that awareness raising, education and technical support to prevent e-crime is essential, but that this must be done in such a way that we do not frighten people or discourage them from developing e-business or other e-applications.

We will raise awareness, not fear.

The workshops highlighted that many companies and individuals are largely ignorant of security issues and the need for any sort of security measures on-line at all. Many displayed an "it won't happen to me" approach to e-crime.

Many individuals expressed their ignorance of the scale of the current threats and it's potential impact on their business and systems.

The steering group recognised that to achieve buy-in from business and other stakeholders, then a clear sustainable and long term action plan was required. Actions being concrete and practical with clear assignment of responsibilities plus clearly defined benefits for all.

Working closely with already established police posts such as Business Liaison Officers we are now running awareness days for business users - talking through the issues previously raised at the workshops and summit, in order to reinforce the crime prevention messages and to instigate self-help groups.

During the summit there were frequent references to the lack of accessible and understandable security information. People simply do not know where to go when they experience IT problems, let alone IT security issues. Furthermore there is a perceived lack of adequately trained and trusted people to provide the advice. The open days for business is a huge step forward in addressing this problem.

There is also recognition of the need to raise awareness and education within the Police Service in Wales and within our partner agencies. We have now begun an Awareness Raising Module within North Wales Police to our Probationary Constables (new staff). This will be monitored and evaluated and cascaded to other forces around Wales.

The purpose of the E-Crime Summit was to address the threat of e-crime in Wales, which currently costs businesses in Wales in excess of £160 million per year. The recommendations of the summit have been reviewed by independent consultants and academics and have now formed the basis of a 'Manifesto' for Wales, outlining the priority areas, the partnerships required and the interventions needed to tackle this problem.

The steering group commissioned specialists to produce a costed action-plan, with clear short, medium and long term objectives and targets for delivery to the business communities across the whole of Wales.

The Action Plan will be launched by the Welsh Assembly Minister for Economic Development and Transport in July 2005.

The Welsh Assembly Government have acknowledged that the Summit was the stepping stone to leading the way in tackling e-crime and would pave the way for Government, Business and Law Enforcement Working in this critical arena.

Following the July 2005 launch of the action-plans a more structured and supported delivery of service will be available to ensure resources are accessible to assist with advice in setting out security policies for SME's. We will also be better equipped to set some Common Practices and Standards, a version of the British Standard for Information Security Management, BS7799, capable of being understood and implemented by the smaller businesses.

Over the past 12 months the Multi-agency Steering Group has achieved much in raising the crime prevention campaign against e-crime in Wales, with many other regions around the UK now seeking advice and assistance in order to put into action the best practice, identified and adopted by the Welsh Region.

A full synopsis of the Workshops and Summit has been prepared and disseminated to all delegates – a newsletter giving updates of, where we are now, is due to go out May 2005 and a series of open day, follow-up, business forums is underway to ensure that we keep up the momentum and enthusiasm in our bid to “combat serious and organised hi-tech crime, making Wales a safe place to live and work”.

The Steering Group will remain in being and will monitor and evaluate progress, with designated areas for responsibility to the group members to ensure appropriate progress is being made in line with set objectives and agreed action plans.

An E-Crime Summit (2) will again be re-launched in February 2006 to strengthen working relationships, obtain feedback, adjust action plans accordingly and to reiterate joint-ownership and true crime prevention partnership working.

Please see attached appendices.