

Goldstein Awards 2019

Application Form

**DS Lucy Edgeworth
PC Lloyd Nethercott**

**Avon & Somerset Police
United Kingdom.**

Summary of application

Scanning:

Cyber-crime is a tier 1 threat to the country and the average offender age is 17. A national Cyber Prevent network was created to deter individuals from getting involved in cyber-crime or moving deeper into it. Young people lacked knowledge on the law and their cyber skills often outmatched their teachers. This led to young people being drawn into hacking offences.

Analysis:

When analysing cyber dependent crime, we found:

- No set location for victims as anything internet enabled is vulnerable. Due to the age range of most offenders (young people), concentrated efforts would be needed in educational establishments.
- The majority of offenders start their pathway at school age, usually through interests in gaming or technology and progress through independent learning or wishing to prove themselves.
- Victims will vary from large commercial businesses to individuals.

Due to its 'invisible' nature, the best way to target cyber-crime is to prevent it from happening in the first place.

Response:

We built 'Cyber Futures' (CF) on three pillars:

- Inform – Provide those at risk with information to make ethical decisions and equip others to identify individuals at risk.
- Engage – Work with others to provide advice and better understand reasons behind involvement in cyber-crime.
- Inspire – Inspire individuals to use their skills lawfully and ethically, enabling brighter cyber futures.

We worked collaboratively to achieve our objectives in delivering the South West Cyber Roadshow. We established partnerships with education professionals, creating a referral pathway encouraging early reporting of individuals they deem at risk. We also created a remote apprenticeship, the first of its kind, to develop existing cyber skills & provide valuable work experience for referred individuals.

Assessment:

Prior to CF, dealing with individuals committing cyber-crime meant criminalising teenagers without them understanding the severity of their actions. The roadshow proved that student's knowledge around the law was very limited yet greatly improved by the end of the sessions. CF has received positive feedback from teachers, young people, cyber security stakeholders, parents, guardians and other police regions.

Professionals used our reporting pathway, enabling us to carry out early interventions to prevent young people offending. 3 subjects are involved in the remote apprenticeship, some performing above post-graduates. Our understanding of pathways into cyber-crime has grown, enabling our product to remain agile and prevent offending further by giving those at risk the knowledge to do the right thing in the right way for the right reasons.

Number of words: 392

Description of project

Scanning:

Over the past decade the world has seen massive technological advances. Nearly every organisation, company and government agency relies heavily on the interconnectivity of our world to go about normal everyday business.

As with any aspect of society there will always be those who wish to cause harm and cause disruption and we have seen a great increase of cyber enabled and dependent crimes over the past few years. Cyber security is a real risk to our society and as such was identified as a Tier 1 threat in the 2010 National Security Strategy, alongside Terrorism, War and Natural Disasters.

The National Crime Agency (NCA) started to look in more detail at the young people becoming involved in cyber dependent crimes and in 2017 produced the paper 'Pathways Into Cyber Crime' which contained key recommendations.

Across the country Regional Cyber Crime Unit's (ROCU's) set up Prevention officers in order to assist in delivering on the objectives set by the NCA which were:

To deter individuals from getting involved in cyber dependent crime in the first place, moving deeper into cybercrime and to prevent reoffending.

In order to deliver on these objectives it was clear that we needed to fully understand the problem to be addresses. Research by the National Cyber Crime Unit (NCCU) explains that the average arrest of offenders for this type of crime is 17 with many stating they started this activity at 12. (Crest. Identify, Intervene, Inspire. 2015).

It was evident that we needed to engage with our target audience – young people.

On speaking with our own Pursue team it was clear that the consequences of being drawn into this type of crime were great - young people were ending up with criminal records and interactions with the police for serious offences.

With no local, national or international borders with cyber it was evident from a stakeholder analysis that there was a vast amount of businesses interested in cyber security but a limited amount in the prevention of those being drawn into a life of cyber-crime.

We conducted an overview of all 5 police forces in the South West which identified no preventative work in this area. We identified key stakeholders who had an interest in this area and communicated with them. Stakeholders included the Cyber Security Challenge (CSC) who were able to tell us that they had evidence of an emerging amount of talented children who had no idea about the Computer Misuse Act.

The National Cyber Security Centre (NCSC) are keen to develop cyber skills in schools and also reported that the ethical implications of online activity are not out there. BlueScreen IT (a cyber security business) reported seeing vast amounts of young people on the periphery or having committed CMA offences.

Initial contact with local schools also identified an emerging trend in children whose skills in cyber out skilled the teachers and a significant amount of network intrusion had not been reported.

Overall a vast amount of stakeholder's had an interest in reducing offending and in offering positive pathways for young people.

What was also interesting was the lack of research into the problem within the area where our target audience was - educational establishments.

Analysis:

We broke the problem down by creating 'Key Performance Indicators' – KPI's. These allowed us to establish what success would look like. We mapped these KPI's on a time line for most important to least important and from this Cyber Futures was born.

It was clear from our initial research that there was a lack of understanding about the crime from every angle – the offenders, parents, schools, police, youth offending teams and contributing to this was the lack of positive pathways available for young people to practice their skills ethically and legally.

Problem Analysis Triangle:

Using the Problem Analysis Triangle (PAT) it was evident that cyber dependent crime was quite different to traditional crimes, there are no sociodemographic boundaries and were often being committed by teenagers in their bedroom. The absence of a guardian was not necessarily the case – more so that the guardian or parent have no idea of what their children are capable of doing via their computers in their bedrooms. "But he's in his bedroom, he's not out on the streets causing trouble".

The crimes committed can vary significantly – from 'booting' a friend off a game you are playing on-line to causing a multibillion dollar company to shut down for a few hours (both crimes committed by teenagers in the South West).

Prior to Cyber Futures there was no preventative work being done by law enforcement in this area of crime, it was vital that we changed that.

By applying the PAT we were able to look closer at the problem and identify the contributing causes.

Location:

Unlike traditional crimes Cybercrime spans over homes, business, government – in fact anything and everything that is internet enabled. Although millions is spent every day across the globe on cyber security, breaches still occur. However taking the research into account it was clear that a good location in which to concentrate this preventative work was in the areas highly populated by the offending age group – education establishments.

Suspect:

Previous research, and our own criminal cases, identified that the majority of offenders started around school age. There is a clear progression of young male game enthusiasts who become involved in coding to modify games that may move towards more serious crimes on line. Previous research also suggested that offenders had a deep interest in technology and were often academically gifted. Research looked into why young people become drawn into this type of crime and sighted was "a way of acquiring power", "a sense of belonging", "desire to prove yourself" (Crest. Identify, Intervene, Inspire. 2015). Research is also being conducted by Bath University looking at the links between those with Autistic Spectrum Disorders (ADS) and those who commit cyber dependent crimes.

Victim:

Victims vary from large commercial businesses to the individual gamer.

It is worth pointing out that cybercrime will not be defeated by law enforcement detection, due to its global nature and its intensely personal delivery (i.e. that most victims are targeted without even knowing it until it's too late). The best way to target this type of crime is to prevent it in the first place and to educate victims (as it being done by numerous campaigns such as 'Tell 2' 'Little Book of Cyber Scams', in house cyber security training.)

We need to educate the 'could be' and 'would be' offenders and find them positive pathways and an environment in which to practice their skill lawfully.

Previous responses to the problem have always been to deal with the crimes after they occur, both in a formal setting and informal setting – for example:

Goldstein Application: Cyber Futures

A boy in the South West hacked into his school network and viewed teacher's private emails. The boy was expelled, arrested, had his home searched and convicted. He had no previous dealings with the police before then. The conviction negatively impacted his life moving forward.

On speaking with educational establishments it was clear that teachers were simply not aware of the law surrounding the cyber space. It was also clear that even the computer science teachers had little to no knowledge in this area. It simply wasn't part of the curriculum. This also meant that they had no means by which to identify and support students who were vulnerable to being drawn into this type of crime.

Parents reported that their children often out skilled them when it came to technology, often reporting that they find it difficult to protect their children and offer them advice in areas they have little to no knowledge. Some very talented children are also being dissuaded from following what could be an excellent career pathway by parents and teachers who are worried about their children's activities in the cyber world.

At no point was anyone providing the young people with any input on cyber ethics – 'Doing the Right Thing in the Right Way for the Right Reasons'. No positive pathways were being shown to young people

Response:

We created, designed and developed the Cyber Futures Initiative. This was initially an engagement platform and tool for education establishments but has since developed as the cornerstone of our cyber prevention work. Cyber Futures is formulated around 3 key pillars:

Inform: Making sure people have the information needed to make informed, lawful and ethical decisions around their cyber activity and equipping others to identify those at risk of committing Computer Misuse Act offences.

Engage: Working with others to provide advice, interventions and positive pathways, and to understand how and why people are drawn into committing these types of offences.

Inspire: Inspiring people to use their cyber skills lawfully and ethically, enabling them to have bright Cyber Futures

Cyber Futures is an agile product which looks to continuously improve; change is embraced and feedback sought. This allowed for the short development cycle and allowed the SWRCCU to deliver a product quickly.

Under the Cyber Futures umbrella we responded to the problem in the following ways:

- **South West Cyber Roadshow and creation of referral pathway** and template for other forces and regions:

Our aims here were:

- Engagement with young people to inform them of what the Computer Misuse Act (CMA) is and how this translated into everyday dilemmas that they may face, along with the consequences for them and others in making the wrong decisions. We also recognised that we could provide advice and interventions, offering positive pathways for those who want to, and have the skills to have a future in the Cyber Security industry.
- Engagement with teachers, safeguarding leads and network technicians to highlight the objectives of the Cyber Prevent strategy and offer them advice, guidance and support in this area.
- Highlighting the importance of sharing information to support individuals at an early stage by way of the creation of a suitable referral system and using our Support Request Form (see appendix 1.0).

We had established that there were other stake holders working within the South West around Cyber. On liaison with these organisations it became evident that a group of us could work together to achieve our

Goldstein Application: Cyber Futures

own objectives under one programme of work – namely a South West Cyber Roadshow. In February and March 2018, together with Cyber Security Challenge (CSC) and Computing At School (CAS), we embarked on the Roadshow. We aimed to ensure the delivery of the Prevent message and to establish working relationships with education professionals in order to encourage the early reporting of young people they deem at risk of being drawn into Cyber Crime. A specific referral pathway was mapped out with schools knowing how to highlight a young person in need of intervention. Overall, 11 educational establishments received an interactive Cyber Ethics and Legislation session.

- **National Cyber Security Centre (NCSC) Cyber School Hubs**

Following the success of the Cyber Futures Initiative we were contacted by colleagues at NCSC (GCHQ) who are addressing the current cyber security skills gap and are piloting Cyber Schools Hubs – we are official supporters of this and have delivered our ethics session to numerous bespoke audiences.

- **Remote Cyber Apprenticeship's**

We created our own positive pathway for young people we had cause to deal with under Prevent. This was for young people who were very talented in cyber security, at risk of offending due to their learning and who otherwise weren't likely to achieve in a traditional academic sense (our main target group). We established a partnership with a South West cyber security company (BlueScreen IT) and created a 'first of its kind', remote cyber security apprenticeship. This meant we could use the pathway from a wider geographical area utilising BlueScreen's remote working and learning platforms. Apprenticeships are not new however we realised that there young people who might not be ready to move away from their homes but could still excel in this area by completing a remote apprenticeship. This positive pathway requires buy in from not only the apprentice but those around them (parents/ guardians). We placed two young people on the new initiative as a pilot.

- **Cyber Futures Inputs**

Following on from the Roadshow we have delivered our Cyber Futures inputs to over 3000 young people to date with a huge majority confirming they now know more about how to practice their skills ethically and lawfully than they did before our input. These inputs have also allowed bridges to be built between education establishments and law enforcement with over 30 referrals for extra help to date.

- **National Crime Agency (NCA) Intervention Workshop pilot**

We hosted and assisted in the organisation of the NCA's intervention workshop aimed at deterring those who had either broken the law or been on the periphery of committing the crime. We provided inputs for the young people and for the parents and guardians.

- **Interventions**

We have provided 16 Cease and Desist interviews to date – these allow us to say to young people that we are aware of what they are doing and this is their opportunity to stop. We also explain the Computer Misuse Act to them and signpost them to safe and lawful places to learn and practice these skills. From a law enforcement perspective, these also allowed us to evidence the fact that these young people knew what they were doing if they chose to reoffend.





Goldstein Application: Cyber Futures

Assessment:

Prior to Cyber Futures being set up the only way to deal with individuals who had committed cyber-crimes was to pursue them and bring them to justice after the crimes had been committed – this meant that teenagers were often being dealt with by the police and justice system with some not even realising the severity of their actions (“I was just messing about in my room... I didn’t really think about it”). There was very little preventative work going on.

The SW Cyber Roadshow allowed us to work with others and target specific audiences enabling an effective and efficient delivery of our objectives.

Ideograph showing overall results of Cyber Ethics and Legislation sessions:

	11	Schools received a Cyber Ethics Input
	22	Cyber Ethics Sessions delivered
	81	Scenarios of CMA offences were given
	424	Students took part in the sessions



67%

Responded with answers that meant they would commit a CMA offence.



27%

ASD school students responded with answers that meant they would commit a CMA offence.



Following a debrief and input provided by SW RCCU officers:

90%

of students voted that they "know more about computer law and how to practice your skills legally than before this session."

Goldstein Application: Cyber Futures

As can be seen in the ideograph above; 12 schools received a Cyber Ethics and Legislation input. Of these 12, 3 had additional schools attend their cyber days and 2 did not form part of the roadshow (they were specific sessions for cyber days).

Overall, a total of 22 Cyber Ethics and Legislation sessions were delivered to a total of 424 students aging from 11yrs to 18yrs.

In total, 81 ethical dilemma scenarios were given.

67% of students responded with answers that meant they would commit a CMA offence if placed in a given scenario.

The motivation behind their decisions to commit these crimes was interesting and documented (full details in the SW Cyber Roadshow Report).

Students had little to no knowledge of CMA offences or of the scale of the possible punishments under the legislation.

A real emphasis on the doing the Right Thing in the Right Way for the Right Reasons was given to the students, explaining that they may find themselves in difficult situations where they may be pulled emotionally, ethically and morally and have the cyber skills to cause harm and disruption but that their decisions could impact on the rest of their lives and others. The Right Way was explored and students were encouraged to think of alternative ways to resolve the scenarios without committing offences.

On conclusion of the Cyber Ethics and Legislation input, 90% of students stated they know more about computer law and how to practice their skills legally than they did before.

The Cyber Security Challenge ran a Survey Monkey following the conclusion of the roadshow. They received 10 responses from teachers, activity providers and speakers. In relation to the Cyber Ethics session they were asked a set of questions:

1. Regarding the Police delivery of their cyber ethics session, was the interactive delivery method effective at engaging students.

For those who sat in on the sessions 100% of respondents stated it was "very effective"

2. Regarding the Police activity, do you think the session provided students with the information to practice their cyber skills safely and lawfully?

90% of respondents stated "yes" and 10% "somewhat".

3. Following on from your contact with the Police officers, would you feel comfortable contacting them for advice or support with students practicing these types of cyber skills?"

100% of respondents stated "yes".

Following our interactions with teachers, safeguarding leads and network technicians a total of 14 individuals were identified to us as needing some sort of further police interaction in order to stop them moving deeper into cybercrime. These ranged from students who have intruded onto the schools network, hacked into student management systems, or who are of concern to teachers with their cyber skills. Some of these students clearly have a high skill levels.

Small selection of Qualitative Results:

Positive Feedback from students following our interaction included:

"Thank you for making this a really fun experience for us! We learnt a lot of very interesting facts"

"I loved this session"

"This was a great presentation. I have learnt a lot. Love the concept with the scenarios and the talk."

"We now have a better understanding of how serious it is to commit a cyber offence, and what the consequences could be."

"Amazing well done it was great"

"The presenters were interesting to listen to and very enthusiastic. The talk was informative and beneficial to our understanding. Thanks!"

"Very interesting session. We enjoyed the interactivity."

Constructive feedback from students following our session included:

"Very beneficial. Don't go into too much detail as someone may get interested"

"Some vids would be good but it was fun"

"Needs more entertainment. Explain more on the computer misuse act"

Goldstein Application: Cyber Futures

Positive Feedback from teachers/ professionals following our interaction included:

"I was really impressed with your session at the UTC on the CMA and the ethical questions posed. We both found it very engaging, hence wanting to vote online (and that is from two government employees who go through a huge amount of legal training). I really liked the format and the way it was delivered, you could tell you had both put a lot of thought into the structure of the session. Your freebies are much better than the Cyberfirst ones also – my phone holder was borrowed very quickly by my 13 year old son when I got back home."

Glenn H

NCSC - National Cyber Skills Delivery

"I thought your presentation was superb and in truth should be delivered to school assemblies as all young people need to be made more aware of the dangers associated with being active online. Ignorance of the law is no excuse and the examples you used during your workshop were both engaging, informative and thought provoking for the students. Students, parents and teachers really need to be aware of this in our digital age."

Elaine Brown

Enterprise and Skills Project Manager

University of the West of England (UWE Bristol)

"Thank you very much for coming along yesterday, you made legislation interesting for students!"

Rich Williams

Head of Faculty

Cyber Security & Digital // SGS Berkeley Green UTC

"The scenarios make the CMA more lively"

Beverly Clark - CAS lead SW.

"Excellent scenarios, really good"

Matt Standing – Henbury school

"Thank you so much for all your hard work on Friday. The students really enjoyed the sessions and it was extremely relevant to their exam preparation. The stories will help the students remember key facts and bring the legal side to life and avoid any misunderstandings."

Sophia Elliott

Beaufort Co-operative Academy

Special mention:

A week after completing one of the sessions we received an email, in order to respect anonymity some details have been removed but the majority of the message remains.

"Hi there,

I just wanted to email and say that it was really good to have met you and the team the other day when you came into my school

Can I just emphasise the importance of what you're doing here, I really feel that up until now there has been no - one looking out for people like me and was pleasantly surprised when I told you about certain things I was able to do with computers as you embraced my passion and spoke to me more about the future and possible other intervention sessions that might be taking place in the future regarding more focused groups of people who are maybe seen as having a hidden talent with computers.

I honestly felt that had I not been met by you and your team that came into our school and talked to separately as someone who needs guidance on what to do next with my skill I would have gone down an entirely different path.

The fact that we have someone like you engaging with us on the ground and not demeaning us for anything we might have done wrong in the past means that people like us will definitely be more willing to get involved with any other activities and step away from any of the darker stuff we might have been thinking about.

I think the key thing is that people with these sort of skills don't know what to do with it. But when you came in and told me of different career paths and possible opportunities to maybe practice and learn more about cyber security, it was a great relief to hear. If you are ever able to organise and setup hack labs for identified people within cities (by having maybe gone round to other schools and heard from people who may have a special talent) then it would be great for people like me to be given a place where we can safely do so. Otherwise I am seriously worried that, like me, others will eventually get stuck and have start committing real world attacks for the thrill of it.

Your company has done a great job and I was so grateful for your visit - Thank you so much."

This email demonstrates the importance of the overall strategy, making a difference to young people's lives to ensure they have bright cyber futures rather than criminal ones.

The results demonstrate that the interactive nature of the Cyber Ethics session was well received by both students and professionals. Student's knowledge around the CMA and consequences of committing offences under it was very limited prior to the session and greatly improved by the end of it.

Goldstein Application: Cyber Futures

Teachers welcomed the assistance and commented on the Support Request Form being a positive thing. The CSC Survey Monkey demonstrated that following our contact teachers would feel comfortable contacting us for advice and support with students who are practicing cyber skills to the point of concern. This is further evidenced by the referrals received.

The interactive sessions were an effective delivery tool for young people who enjoyed the teaching style, the debates the scenarios raised and the use of the tablets to vote live.

The sessions for professionals were vital, allowing for credible working relationships to be formed and referrals received.

NCSC Cyber Schools Hubs – To date we have delivered over 15 **Cyber Futures sessions** alongside the NCSC as part of the Cyber Schools Hubs Initiative. Results are similar to the roadshow with young people stating they know more about computer law and how to practice their skills legally than they did before. In March 2018 The South West Regional Cyber Crime Unit won the NCSC Industry Champion award and were awarded prestigious ‘Partner’ status due to the Cyber Futures initiative.

Remote apprenticeships – We currently have 2 individuals who are employed by BlueScreen IT as apprentices on our pilot. It is clear that in order for these to be successful young people need the support from those around them – parents, guardians, without that support it’s likely that the young person will not have the environment in which to flourish.

The apprentices are both doing very well, gaining industry recognized accreditations and work experience. One was interviewed by the BBC recently where he explained how he feels about this opportunity. This young man has turned his life around. Another has visited a large cyber security company for a day as part of his work experience and feedback from this was that he was outperforming their graduates.

NCA workshop – We delivered our Cyber Futures input to both the young offenders and a separate session to their parent/ guardian.

One of the young offenders wrote:

“I am emailing you just to say a huge thank you for inviting me to the cybercrime intervention day, I thoroughly enjoyed myself and found the whole experience to be hugely beneficial.”

A Probation worker, who attended with a young offender wrote:

“I found the day really informative and positive. **** said that he enjoyed the day and found it helpful. In our session on Monday, we went through which bits he liked and which bits he did not like. He said there was there was nothing that he did not like about it, even the journey!... we spoke about all the different avenues he could re-search.”

Mo Batsel

Youth Justice and Prevention Worker

Interventions - Under Cyber Futures over 16 Cease and Desist notices have been delivered and full intelligence de-briefs conducted, allowing us to paint a clearer picture around who our cyber offenders are. Interventions have also been through highlighting of positive pathways (such as Capture the Flag exercises run by CSC, Immersive Lab’s training environments, the NCSC’s Cyber Discovery Programs).

The Cyber Futures Initiative is about Informing, Engaging and Inspiring young people to have bright Cyber

Goldstein Application: Cyber Futures

Futures.

It has had positive feedback from teachers, young people, cyber security stakeholders, parents, guardians and other police regions.

Because of its rather unique situation, unlike traditional crimes where you are simply trying to tell people not to do 'it', hacking can be something that ruins your career prospects OR grants you access to a very lucrative and positive career. Our intention was to displace these young people, away from straying towards committing crime and closer to using their skills for positive reasons.

The truth is that many young offenders under the CMA really didn't want / mean to offend. It's a tough subject to learn with grey areas found at every turn. We feel that cyber futures has been able to remove this grey area for the many young people we have interacted with and thus greatly reduced their desire and /or risk of being drawn into offending.

Number of words: 3495