CREST

Identify, Intervene, Inspire

Helping young people to pursue careers in cyber security, not cyber crime

NCA
National Crime Agency

Executive Summary

Recent events have provided evidence of the extent to which young people can become involved in cyber crime. In September 2015 representatives from CREST member companies met the National Crime Agency's National Cyber Crime Unit (NCA NCCU) at a workshop designed to assist the NCCU's efforts to prevent young people being tempted to participate in illegal online activities.

The workshop was convened as part of NCA work to strengthen the NCCU's Prevent campaign, which targets young people and aims to explain clearly to them what is illegal online, while raising awareness within this group of the potential consequences of cybercrime for victims and for perpetrators. A second aim of the campaign is to highlight the benefits of an interesting and rewarding career in the technical security industry or the wider IT industry that could lie ahead for talented individuals who use their technical abilities for legitimate purposes.

The NCCU wanted to draw on the experiences and knowledge of the workshop attendees, in order to improve its understanding of the characteristics and motives of young people who might move from being interested in coding and gaming into hacking and other illegal activities.

The workshop participants were able to offer some validation, but also some practical criticism, of the methods already being used by the NCCU to identify young people participating in illegal online activity and to contact, advise and support those individuals and their families, carers and/or teachers.

CREST and the NCA will now work together to plan collaboration on knowledge and resource sharing to further the aims of the campaign; and to establish relevant intervention points to try to direct young people away from crime into exciting and worthwhile careers in the cyber security industry. This may include further workshops, CREST contributions to NCCU publicity campaigns, further efforts to identify those at risk as early as possible; and the establishment of a mentoring scheme, with individuals working in the technical security industry offering guidance to young people identified by the NCA as being at risk of falling into illegal activity.

This discussion paper provides some detail about the findings of the September 2015 workshop, but it is also intended to stimulate further discussion and debate within the technical security industry and beyond, regarding additional actions that could be taken to further the goals of the NCCU's campaign. Both CREST and the NCA would welcome further input from readers of this paper.

Workshop discussions and findings

Purpose of the workshop and ongoing work in this area

The workshop was opened by CREST President Ian Glover, who explained the fundamental aims of the NCCU and CREST programmes that the workshop was designed to support: to identify young people who could be tempted to become involved in cyber crime: to stop them committing crime, but also to encourage them to use their skills for positive purposes.

The NCCU's investigations to date suggest that many of the young people who are to be targeted by the NCCU campaign are male gaming enthusiasts. It is possible to see a clear progression that some individuals take towards participating in illegal activities: they become more interested in coding, then in modifications of computer games. They may then join an online coding club and at some point gain a deeper understanding of how they might use their skills for hacking.

At some point the idea that it may be desirable to access or steal certain pieces of information for a perceived common good is introduced, possibly by peers, possibly by other individuals who may have ulterior motives for doing so. As young people become involved with other online coding or hacking forums they may be identified by individuals or groups involved in cyber crime who start to 'groom' them to encourage them to participate in illegal online activities.

Figure 1 illustrates this pathway, progression towards illegal activity and away from a dominance of real world relationships in an individual's life towards a growing influence from online contacts; and the extent to which parents, carers and teachers understand or encourage specific online activities.

Pathway to illegal online activity

Figure 1

Recent events have revealed examples of individuals who may have followed this pathway and become involved in serious cyber crime incidents. CREST's leadership believe it is vital to identify and communicate effectively with young people who might follow this pattern at the earliest opportunity. They should be encouraged to participate in legitimate competitive activities that could offer them prestige and reward, such as the Cyber Security Challenge (cybersecuritychallenge.org.uk) and other events or programmes such as cyber camps, or university or industry mentoring programmes. In a world where young people are – rightly – being encouraged to learn more about coding and about technology in general, the opportunities for a greater number of talented individuals to be tempted into criminal activity will surely continue to increase.

During the September 2015 workshop the participants discussed their own backgrounds, the origins of their own interest in technology and their career paths to date. Almost every participant said that at some point in their lives someone had made an intervention of some kind that had helped them to move into the cyber security industry; and that without this intervention they may not have realised that such a career was possible. Some suggested that they might otherwise have been tempted to participate in illegal activity online.

Many cited the importance of role models, at school, in their personal lives, or early in their careers, who had proved to be positive influences, recognising their interest or talent and helping them to find the path that eventually led to their current roles. Many also acknowledged the importance of education in helping them enter the technical security industry. Two participants had entered and performed well in the Cyber Security Challenge.

The content of these discussions provided some validation of the work of the NCA in this field to date.

NCCU progress to date

The Prevent campaign forms part of the NCA's 'four Ps' approach to fighting cyber crime. The organisation aims to:

- **Pursue** individuals, groups and larger organisations involved in creating the most serious cyber threats to the UK;
- **Prevent** individuals becoming involved in cyber crime;
- **Protect** businesses and the public from cyber crime;
- and to help the UK's business and other organisations **Prepare** to respond effectively to major cyber attacks and to mitigate their impact.

The primary purpose of the Prevent campaign is to deter individuals from becoming more deeply involved in 'cyber-dependent' criminal activities, such as illegal hacking, designing malware or virus writing. Unfortunately, at present there are many opportunities to perpetrate cyber crime, while it is also easy to understand why individuals might perceive low level involvement in illegal online activities as being a low risk activity that can be conducted under cover of anonymity. There also appears to be a common view that cyber crime is a 'victimless' form of crime. The Prevent strategy is designed to overturn both of these perceptions and to increase an understanding of the risks and consequences, for both victims and perpetrators, of these activities.

The NNCU team's work on Prevent to date has included sending 'awareness' letters and/or emails to young people who have registered their details on websites where illegal activities are encouraged, organised, promoted or celebrated. These letters inform the recipient that the NCA is aware of their activity and remind them that the website is involved in illegal activity. It outlines some of the consequences of cyber crime for victims and perpetrators and also encourages recipients to consider taking part in legitimate activities designed to test their skills, such as the Cyber Security Challenge. In other cases the team has visited the homes of these young people to talk to them and their parents or carers directly. There have also been a number of arrests as a consequence of the NCCU's investigations.

The NCCU is also working with behavioural scientists in academia, both as a means of improving the team's understanding of why people are tempted to take part in illegal activities; and of suggesting possible methods that might be employed to dissuade them from doing so. Through this combination of activities the NCCU aims to disrupt the market for illegal online activity, reducing both supply of, and demand for, the skilled individuals who criminals might otherwise seek to exploit or recruit.

In order to explain who is most likely to be targeted by NCCU Prevent activity, individuals involved in illegal activity can be imagined as being members of groups within layers of a pyramid (see ***Figure 2***). At the top are the smallest group, the most serious cyber criminals. A second level would include malware developers and senior hacking forum members. Lower levels of the pyramid include RAT or Stresser users, with the lowest groups in the pyramid including members of hacking forums and gaming enthusiasts who may be experimenting with hacking.

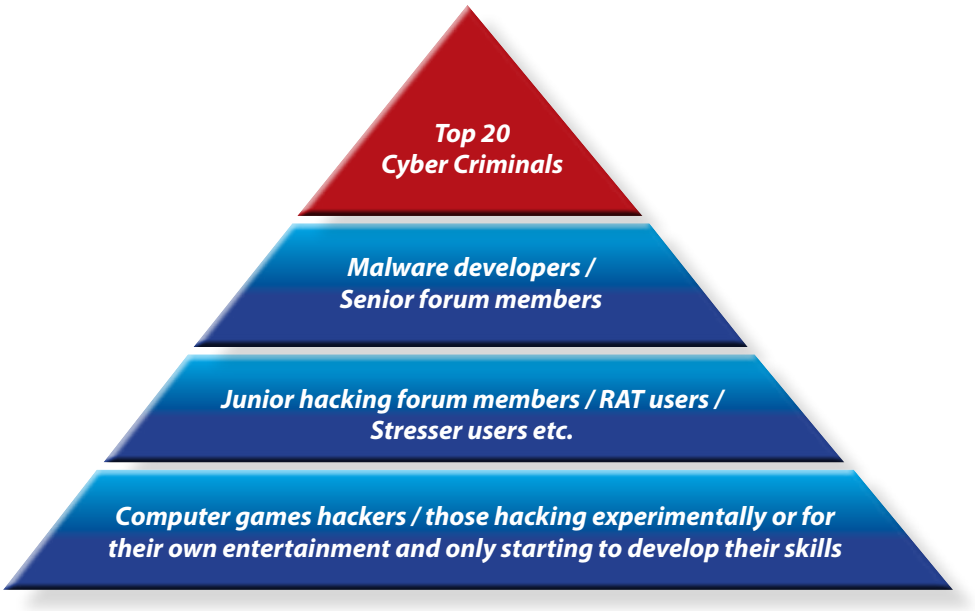


Figure 2

The NCCU may identify, communicate with and if necessary arrest individuals operating within any of the levels within this pyramid. Individuals in the lowest group are more likely to be the target of Prevent activity. Individuals within the groups higher up the pyramid are more likely to be actively pursued by law enforcement agencies, but many of the individuals who start at the lower levels could rise towards the higher levels rapidly, so could also face arrest. The NCCU's approach is based on identifying these individuals as quickly as possible and intervening, either to prevent them from becoming more involved in illegal online activity or to stop their activities immediately if they are already involved.

The NCCU's research to date suggests that individuals at risk of becoming involved in illegal online activity may be as young as 12. They are likely to have a deep interest in technology, often first sparked by an enthusiasm for gaming; and are likely to spend a large and increasing proportion of their lives online. In some cases when these individuals have been contacted via a home visit, parents and carers are frequently amazed to discover they have been engaging in illegal activity, because they spend so much time in their bedrooms.

These young people are often academically gifted, certainly in terms of achievement in technology and related subjects. In some cases they appear to have started to investigate the intellectual challenges coding and hacking present at least in part because they are not adequately challenged by school or university technology subject syllabuses. Some have been diagnosed with forms of autism or with Asperger's Syndrome.

The NCCU's campaigns to date have clearly had some impact. Evidence from hacking forums shows that awareness of the operation and of the fact that the threat of a home visit from the police was not an empty one seems to have spread fairly quickly. The content of the letters has been very carefully tailored for its most likely audience – there is a need not to terrify the recipients, some of whom may be vulnerable young people, but to persuade them that there are better ways for them to hone their technical skills. A large majority of recipients click on the link in the email that provides further information.

Some of the workshop participants said they found it easy to imagine that these letters would probably at the very least unnerve the recipients and might well put them off continuing at least some of the activities with which they were involved. However, they also pointed out that other recipients might see the letter as proof that they had created a satisfying level of trouble.

> ***"Most people in these groups feel that they're immune from being spied on. I do think an email would freak a lot of them out. In the forums people often talk as if they have unlimited power. If you knock on the glass I think a lot of them, particularly the young ones, would be very surprised and concerned."***
>
> ***(Workshop participant)***

Understanding why young people might get drawn into criminal activity

In the first of the workshop discussion sessions participants considered the following questions:

- How and why do people get involved in cyber crime?
- What are their key motivations, characteristics and influences?
- How do we increase our understanding of these individuals?
- How and why do individuals progress into more serious cyber criminality?

Some participants suggested that some of the young people who are most tempted to become more involved with illegal online activities may be suffering from some unpleasant social pressures in the physical world: they may have been bullied, for example. Some may also have suffered from depression. Some may find hacking appealing in part because it offers **a way of acquiring power.**

It was also suggested that these individuals may enjoy the **sense of 'belonging'** they get through membership of hacking forums and other online communities.

"You are with people who are like-minded. The computer removes race, creed, sexuality. You're with people you can relate to."

The **desire to prove yourself** within these communities was cited as a factor that could lead towards more serious illegal activity. This desire to prove your abilities can lead to individuals creating a 'righteous hack': a way of hacking into an entity that has not been performed before. Such hacks are also often the source of damaging malware.

"Doing a SQL injection will get you some credibility, but a righteous hack will be expected at some point: something that no-one else has done. The point of doing a righteous hack is that it's a challenge. Just breaking in isn't the point – it's about breaking in with finesse."

These individuals may also be strongly motivated by **a desire to improve their own skills**. These are often people who get a great deal of satisfaction out of solving difficult problems.

"There's that thing of getting the next bit of your knowledge – something you can only get if you perform a specific task."

"There's a saying in the hacker world: 'you don't learn to hack, you hack to learn'. You're striving to learn more."

"Hacking is a very creative art. You get addicted to it because by going up the ranks you get more points. People want to know you because you're higher up the food chain. These communities are structured around reputation and getting to the next level."

It seems that **financial gain is often only a secondary motivation**. Indeed, those who simply use their skills to steal money are not necessarily admired within these communities.

"It's more gratifying to know you could do it than it is to actually do it. I've seen hackers steal money, but usually with automated tools. That's just crime, not a hacker being creative to beat the system."

"Information is power. There's an element of money being a little bit crass."

Some young people may also want to use their skills **to further political ends**. Again, it is easy to see how attractive this idea becomes when combined with the chance to gain recognition and notoriety within these online communities.

One participant summarised the motivations of a hacker like this: "If you have a problem to solve, enough time to solve it and someone to prove wrong that will give you a hacker."

Participants suggested that where an individual crosses the line into illegal activity is not necessarily of paramount interest to these individuals. In some cases they may not be too concerned who is paying them or why they are being asked to complete the task. **Often the main motive for doing something illegal is simply that it presents an interesting challenge.**

"It's goal-oriented. If the goal is to get that piece of information then doing it legally or illegally just doesn't come into it."

"You only ask for part of the puzzle. You smell that it's illegal but you just ignore it. You don't really see what's wrong with knocking out some code."

How do we stop young people using their skills for criminal purposes?

In the second discussion session, participants considered the following questions:

- How can we effectively prevent these individuals from becoming cyber criminals?
- What are effective interventions?
- How can we ensure that young people use their skills for good, rather than following a career in cyber crime?

The participants felt strongly that **spreading awareness of legitimate initiatives**, training and events designed to improve and test technical skills could help encourage talented young people to move away from criminal activity.

They also stressed the value of being able to describe to young people the **opportunities and rewards they could enjoy if they pursued a career in the legitimate technical security industry**, or the broader IT industry. With greater involvement from the security industry it should be possible to organise visits to security companies' premises, in order to give the young person a clearer idea of what a career in technical security might involve.

Participants highlighted the potential value of NCCU using its interactions with these young people to encourage them to participate in not just the Cyber Security Challenge, but other national and local coding competitions, events and programmes. The UK Government's Department for Business, Innovation and Skills (BIS) is currently sponsoring work with CREST aimed at establishing a greater presence for the cyber security industry at educational fairs and other events, which should help in this respect.

Some of the workshop participants said that during their own childhood they had been praised by parents who were clearly proud of their child's apparent technical ability – but who also had an uncomfortable feeling about the direction it seemed to be taking.

Participants also highlighted the **importance of role models and education**, emphasising the importance of the roles played by parents, teachers and peers in influencing young people. They recognised that **parents and teachers need**

people who are at risk. In particular, they need to know where to go for support and guidance.

They suggested that an **early intervention** meant there would be a better chance of preventing an individual progressing into more serious illegal activities.

Helping NCCU Prevent become even more effective

Workshop participants were also briefed on plans for the NCA Prevent campaign, which launched in December 2015. The campaigns. The #CyberChoices campaign was aimed specifically at the parents of 12 to 15 year olds and incorporated a multichannel media campaign, including social media and video content, designed to spread clear messages about what is and is not legal and the consequences of cyber crime.

Convicted ex-hacker Ryan Ackroyd and other potentially influential role models will talk about why they have now chosen to use their skills for legitimate purposes and about their experiences of ending up on the wrong side of the law.

Some reservations were expressed by workshop participants about highlighting the experiences of individuals who have been involved with the 'dark side' of IT, because it was feared this would suggest or reinforce the perception that taking part in such activities can be a legitimate route into the cyber security industry – a view that the industry cannot endorse. The NCA view is that if ex-offenders describe the negative consequences of their past actions this will act as a meaningful deterrent.

The primary targets of the campaign will be parents, teachers and carers of young people aged from about 12 to 19, with the young people themselves forming a secondary audience. Media

partners include the influential online news channel Vice, but the campaign will also make use of mainstream TV programmes to spread awareness of these issues to the parents of young people who might be tempted to get involved with cyber crime.

The campaign launch day included features on BBC Breakfast News and The One Show and had a potential TV audience of 40 million viewers. Video content uploaded to Facebook, Twitter and LinkedIn had attracted 500,000 views as of January 2016. Overall, this is the largest audience ever reached by an NCA campaign.

Further efforts to establish a stronger presence for the cyber security industry at major educational events should also help to further the aims of the campaign. The campaign will also make use of resources created by NCA's CEOP (Child Protection and Online Protection) Command team; and of its network of 'ambassadors' within the education sector, who include teachers and headteachers. Schools will be provided with resources to help plan PHSE [Personal, Social, Health and Economic education] and/or technology lessons within which children will be asked to consider these issues. The NCA has also commissioned research to determine levels of awareness of these issues among the general public.

Workshop participants were keen to share their views on these ideas. They shared the NCA's concerns about the difficulties of communicating effectively with parents or carers of young people who might be at risk of being tempted into cyber crime. The fact that parents' technical knowledge is likely to be much less extensive than their childrens' knowledge was highlighted as a particular problem – although one participant pointed out that when he was involved in similar activities during his youth his mother had no idea what he was doing, even though she had a relatively high level of technological knowledge.

It was agreed that there would be significant value in being able to provide parents with better guidance on how to identify if their children might be involved with this type of activity; and better guidance on what to do if this was the case.

The participants felt strongly that the approach should certainly not be to try to ban the young person from using a computer – although they also agreed that the threat this might happen was an important element in the 'awareness' emails and letters the NCCU is sending to young people found to be involved in small-scale illegal activity. Instead, they felt the focus should be on the potential career opportunities that lie ahead for talented young people in the technical security and broader technology industries. They advocated further promotion of the Cyber Security Challenge and similar initiatives across the UK and beyond, through all available media channels and in schools, colleges and other educational institutions.

It was felt that this type of positive intervention at this early stage in the pathway that can lead to participation in illegal activity would have positive effects. There is a need to create an understanding among the target audiences that moving further along the pathway could have a very negative impact on individuals' future career opportunities within the cyber security or broader technology industries. That means it would be wise to include this message within the influencing emails or letters, even though this would have to be a carefully worded 'soft' statement

Further Actions

CREST representatives at the workshop and the other workshop participants all expressed a willingness to work with the NCA on further publicity campaigns and awareness-raising activities. Member companies would also be willing to consider contributing to mentoring schemes and/ or allowing young people to visit their facilities in order to find out more about, as one participant put it "the cool jobs you can do". This activity could also be extended into/ coordinated alongside internship or apprenticeship opportunities.

CREST has also suggested it might be able to create further Frequently Asked Questions (FAQs) responses to be made available online for young people, their parents, carers, teachers and other interested/concerned parties to consult. CREST is also willing to set up a panel of experts who might be able to respond to direct enquiries on a regular basis. There may be further opportunities for collaboration in relation to other government-funded work already underway at CREST to promote careers in the technical security industry to schoolchildren and students at educational and careers fairs and similar events; and via other channels such as **Imagineering.org** and **inspiredcareers.org**.

Other possible interventions

Further potentially useful interventions and where they might be applied within the pathway towards illegal activity described above are shown in ***Figure 3***, with a key below.

Possible intervention points

Figure 3

Key:

- **A** Provision of better access to information about careers in technical security/IT and online challenge activities for gaming enthusiasts;
- **B** Collaboration with online gaming industry on careers information provision on game packaging and via in-game advertising;
- **C** Advertise legitimate online challenges and provide careers information on online forums;
- **D** Collaboration with online gaming industry on providing clear guidelines on the legality of computer game modifications and careers/online challenge information on sites used by young people seeking to learn/enhance modification skills;
- **E** As part of the major educational schools events programme, creation of an identification criteria to help NCCU ambassadors working in schools spot young people who could be at risk;
- **F** Creation of talent identification criteria and programmes within schools, in order to help teachers highlight legitimate opportunities to improve skills;
- **G** Creation of video and literature content explaining the impact of cyber crime on vulnerable individuals and on jobs;
- **H** Creation of video and literature content for parents and teachers describing the pathway to illegal activity, tips on identifying the signs that an individual is moving along this pathway; and signposting where to find additional support and advice;
- **I** Potential support provided to existing initiatives such as Hacker House;
- **J** Additional funding or sponsorship of educational programmes on conversion courses to lead to recognised qualifications;
- **K** Provision of access to mentoring services, on both a one-to-one and one-to-many basis, provided by CREST member companies and other industry representatives.
- **L** Industry follow-up to the cease and desist notifications and appeals to participate in legitimate activities.
- **M** Further positive marketing activities within hacking forums;
- **N** Promotion of the Cyber Champions network to young people, in part as a way for them to demonstrate their skills to their peers at schools and within their communities.

Request for responses

CREST, its member companies and the NCA are already starting work on some of these intervention points. In order to continue the momentum, develop some of the concepts and identify further possible interventions that could help, additional support from industry and government is required.

CREST and the NCA would each like to encourage anyone reading this discussion paper with further thoughts or ideas they would like to contribute to a discussion of the questions at the heart of this issue to share them.

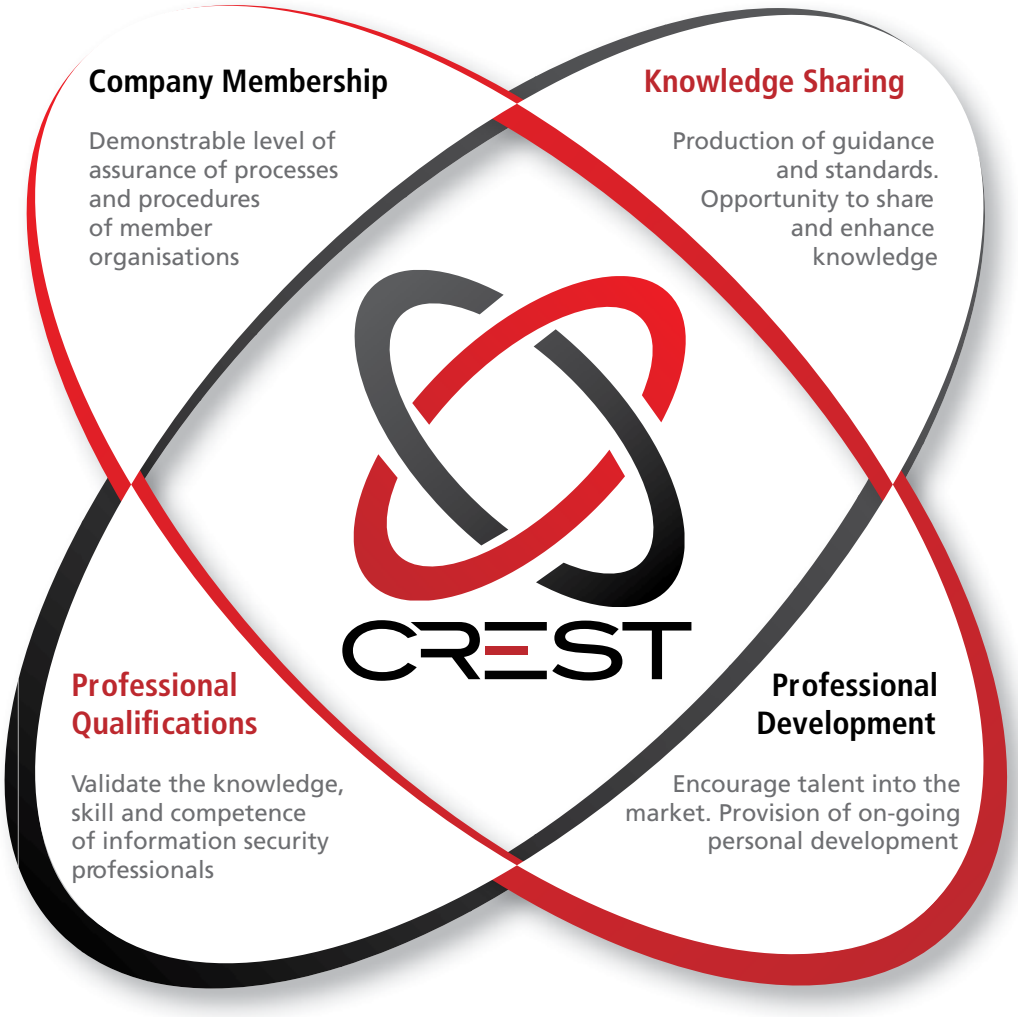
- How do we effectively identify young people who might be at risk of getting involved with illegal activity online?

- What are the best ways to approach those young people, their families, carers and teachers, in order to support them, dissuade them from participating in criminal activities and encourage them instead to find legitimate ways to use and improve their skills?

- And what more could the technical security industry and the broader technology industry be doing to complement the work of law enforcement agencies in this respect?

If you would like to share your views, please contact allie@crest-approved.org

CREST would like to thank the NCA for its support. It would also like to thank representatives of BAE Systems, BT, Context, HP, NCC, PGI, QinetiQ and Sec-1 for their attendance at the September 2015 workshop and the contributions those member companies have made to the production of this discussion paper.



For further information contact CREST at
http://www.crest-approved.org

Warning

This Guide has been produced with care and to the best of our ability.
However, CREST accepts no responsibility for any problems or incidents arising from its use.