Risk Culture Influences in Internet Safety and Security

S. Atkinson[1], S.M. Furnell[1,2] and A.D. Phippen[1]

[1]Centre for Information Security & Network Research,
University of Plymouth, Plymouth, UK
[2]School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia
e-mail: info@cisnr.org

Abstract

The predominant risk culture within the UK surrounding protecting children from online predators has a strong influence on the type of awareness raising activities being promoted for children. As reflected in the terminology in the field, e-safety has moved through Internet Safety to be commonly referred to in child protection circles as online safeguarding. Whether this change in terminology benefits the children is debateable. This paper reports findings from a groundbreaking project involving schools in South West England, which explored young people's perceptions of online risk. It was determined that while their knowledge was sound, there is a need to re-frame the current Internet Safety initiatives to provide more emphasis on encouraging changing behaviour.

Keywords

Internet, Internet Safety, Online safeguarding, Risk

1. Introduction

In an ever-changing, technologically complex world, interconnected technologies provide a pervasive communications backbone (Kennedy, et al, 2008). Many young people grow up accepting this as the norm. These children are surrounded not only by mobile technologies, primarily phones, but also a variety of personal gaming consoles and computers, all with ready access to the Internet.

Bate (2000) suggests that modern technologies are now responsible for raising awareness about the latest dangers. Scare stories can be transmitted around the world in a very short space of time and so Bate's (ibid) inference is that this creates the perception that we live in a dangerous world. Humans have to take responsibility on whether to share anxieties about the latest dangers. In the media, editors determine what gets published, but in the world of Web 2.0 the individual has a personal responsibility on what to blog, share, link or send to others.

Within the home environment, there is a gulf of understanding between adults and children (Staksrud et al 2007). Children are technologically savvy individuals, comfortable with the technologies surrounding them whereas parents struggle. This combination of parental responsibility for the safety and welfare of children in a world promoted by the media to be full of dangers on the Internet, leads parents to the perception that their children are engaging in unsafe activities (Sharples et al, 2008).

Understanding risk is important, allowing for active avoidance of situations that can cause extreme danger or harm. As Furedi (2002) describes, the weighing up of the probability of a risk happening is an informed way of managing that risk. Furedi observes that the fatalistic approach of assuming a risk will happen is eroding parenting skills and impacting child development. The findings from the Good Childhood Inquiry (reported by Bennett, 2007) would appear to be support this.

Parental fear of abduction plays a prominent role meaning children are not allowed outside to play unattended. A fear encouraged by media stories surrounding the abduction of children (Pilcher and Wagg, 1996; Gerrard, 2004; Brook, 2009).

Alongside this parental fear of abduction lies warnings from the media (Panorama, 2008) combined with campaigns about the dangers of online stalking and grooming, such as the CEOP (2007) ThinkUKnow programme. These awareness raising activities focus on a narrow area of child protection and have been seen as a hindrance to teaching young people about safe online behaviour (Sharples et al, 2008).

Initially, this paper presents an overview of the current awareness raising activities both within the UK and Europe, concentrating at those aimed at protecting young people whilst using online technologies. Next follows a description of one part of a research project carried out by the authors, with funding and support from Becta, the British Educational Communications and Technology Agency. This element explored the perceptions of young people towards online safety and security. Finally, discussion will concentrate on selected findings from the research activities as ways of illuminating the influence that the risk culture has on current approaches to Internet Safety.

2. Awareness Raising

E-Safety, Internet Safety, Online Safeguarding have all been used to label initiatives designed to make individuals, with a focus on children, aware of potential dangers arising online. These initiatives focus on a narrow element, that of Internet safety within the Information Security field.

E-Safety was the original terminology used by Becta (2006) in their earlier publications. During the course of 2008 the influence of the Byron (2007) report is more widely felt and this focus is reflected in the change in popular terminology to Online Safeguarding. The change of terminology to include Online Safeguarding was to discourage the dismissing of the issues as being simply a matter of the use of technology (Hillingdon, 2009).

The European Union demonstrates differing levels of online risk to young people, but has tremendous activity for awareness raising (Bauwens et al, 2008). The EU Kids Online project (ibid) describes eight EU countries as being at greater risk than the others. Their suggestion is that the risks arise because there is a gap between the informed practices of the Internet users, the children, and the awareness raising activities from government aimed at the children.

To bring these activities together with any sense of cohesion is a challenge and one which the Insafe foundation (2009) attempts to address. Insafe coordinates activities across 26 European countries who each tailor their awareness raising activities to suit their country. Each of these nodes has their own focus, for example the UK node is CEOP who concentrate on addressing issues around child sexual exploitation online. February 10th is the annual European Safer Internet day when each node is encouraged to hold high profile activities on that day to focus attention on Internet safety. 2009 saw not just the release of a video against Cyberbullying aimed European wide, but also the signing of an agreement between all the Social Networking providers (Europa, 2009).

Within the UK there is tremendous activity by both government and charitable organisations. The Byron (2007) report instigated the setting up of the UK Council for Child Internet Safety bringing together a multi-agency approach of governing bodies and industry. At local government level, Local Safeguarding Children's Boards (LSCBs) have set up e-safety subgroups to facilitate inter-agency training on online child protection issues. CEOP (2007a) mentioned above also use a multi-agency approach, combining UK law enforcement with industry and charity.

Within UK schools, the technical infrastructure is overseen by the National Education Network (www.nen.gov.uk). A consortium of regional broadband providers provides filtering, monitoring and blocking software for the schools in different areas of the country. The infrastructure utilises the Internet Watch Foundation blacklist of potentially illegal websites to ensure that children within schools do not access harmful content.

Charitable concerns also play a prominent role in the Internet Safety field. Whilst the NSPCC combines forces with CEOP, Childnet International (2004) has a focus on producing resources. The early Childnet resources focus on threats from predators arising through young people's use of chat, social networking, instant messaging or other Internet use (ChatDanger, 2004). Later resources expand the remit to include educating about illegal music downloads, threats from viruses and spyware (Sorted, 2006).

A key theme throughout these activities is that of protecting children from predatory behaviour, or blocking them from accessing pornographic content. Blocking and filtering has already been seen to be ineffective (Tynes, 2007; Flemming, 2006) as has education using the fear factor (LaRose et al, 2008). However, what is not quite so evident from these most common activities is a way of encouraging young people into safer online behaviours from the perspective of information security.

3. E-Safety Ambassador Research

A key objective of the research was to explore young people's perceptions regarding online safety and security. This was situated within schools in the South West of England. The primary focus of the initiative was to explore how peer education might be utilised in raising awareness, but that reporting is outside the scope of this paper and the focus here is on risk perceptions and awareness raising.

Prior to engaging with the students in the schools, semi-structured interviews were held with the staff of the school. In all but one of the schools, the key member of staff allocated to the research was the ICT teacher with the remaining school referring the research team to the peer education coordinator.

In total nine discussions groups were held at eight participating schools, involving 202 participants. All but one of the discussion groups were designed to last for fifty minutes and were fitted into the normal ICT lesson carried out during the course of the normal school day. The other school held after school sessions to train their peer mentors and the discussion group was part of that activity.

The discussion groups were divided into key sections so that semi-structured interviewing of the group could be carried out alongside group activities. This was to enable those who perhaps were less confident to be able to share their views. Prior to attending the school a class list was of participants was obtained and part of the presentation included a selection of photographs and quotes gleaned from the participants online profiles.

To explore their perceptions of risks, the participants were asked the following questions:

- What does e-safety mean to you?
- Are there any dangers on the Internet? And if so what are they?
    - A ranking exercise was carried out to ascertain their perception of likelihood of occurrence.
- Who protected them?

Questions were also asked about their awareness of anti-virus procedure. This included exploring their knowledge on how to keep their operating system and anti-virus up to date. Questions were also asked to determine what they knew about secure passwords and safe password practices. Pictures were shown of avatars from a virtual world and participants were asked if they would consider talking to these characters.

To effectively measure the perceptions of risk that the young people demonstrate towards online safety and security, the following measures were deemed appropriate:

- Number and range of risks identified;
- Ranking to ascertain perception of likelihood of occurrence;

- Number of protection mechanisms employed;
- Responses to virtual world characters; and
- Choice of activities to promote e-safety.

4. Findings

Prior to the focus groups, a total of eighty-eight public profiles were discovered with the majority of them on one social networking site, Bebo. One school proved to be an exception, having a class with 100% private profiles, but it transpired that they had recently participated in a local authority education exercise to raise the awareness of Internet Safety in the school.

Twenty-eight of the public profiles advertised email addresses with the words "add me" along with thirty-eight dates of birth. The montages and quotes were able to create a reaction and in one group, participants were allowed to immediately change their profile privacy settings which they took advantage of.

The participants identified a total of one hundred and thirty risks with a considerable overlap. The count of risks highlighted for each school is illustrated in figure 1 below.

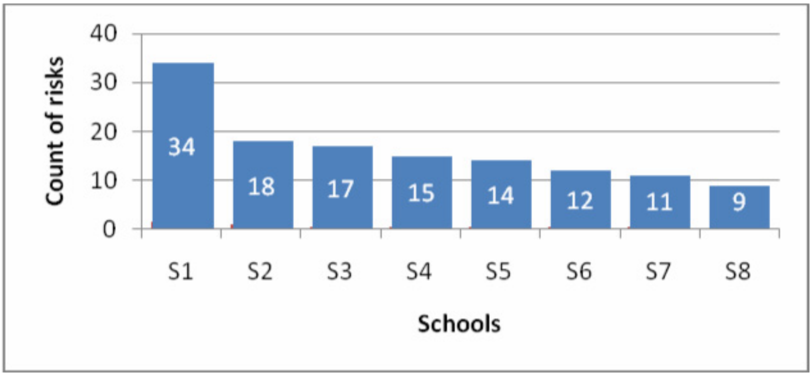

Figure 1: Count of risks

One of the schools here is able to articulate a greater number of risks than the other schools. When taking the number of participants into account as well, two of the schools emerge with a clear specialism in knowledge about online risks, S1 and S2. This was further corroborated by examining the transcripts in depth. The discussions had been dominated in those two schools by some individuals who were able to demonstrate clear and extensive technical knowledge regarding online safety and security.

Figure 2 illustrates the range of risks that were identified by the participants.

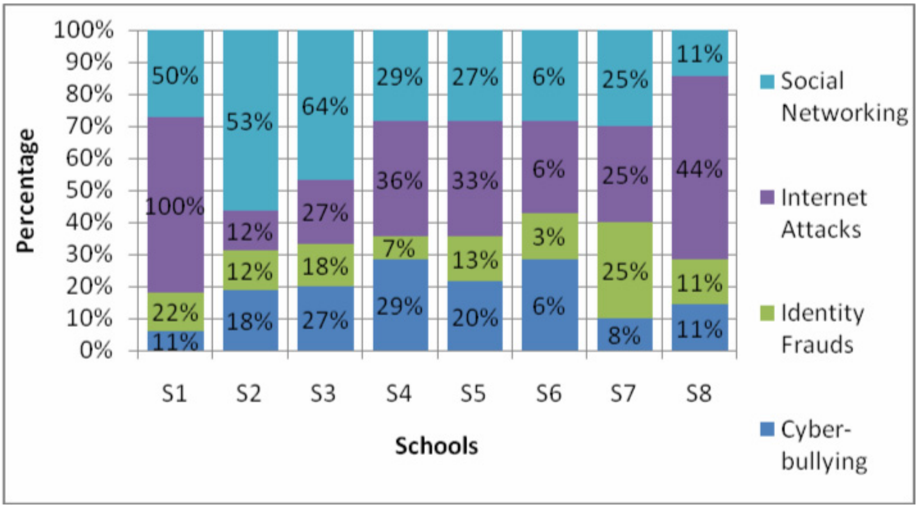

Figure 2: Range of risks identified

As with risks, some schools were able to demonstrate more awareness in certain categories of risk than others. For example, S2 was much more aware of social networking threats that S6.

Following on from the ranking exercises was the perception of risks and their likelihood of occurrence to the participants. Figure 3 below illustrates their perceptions.

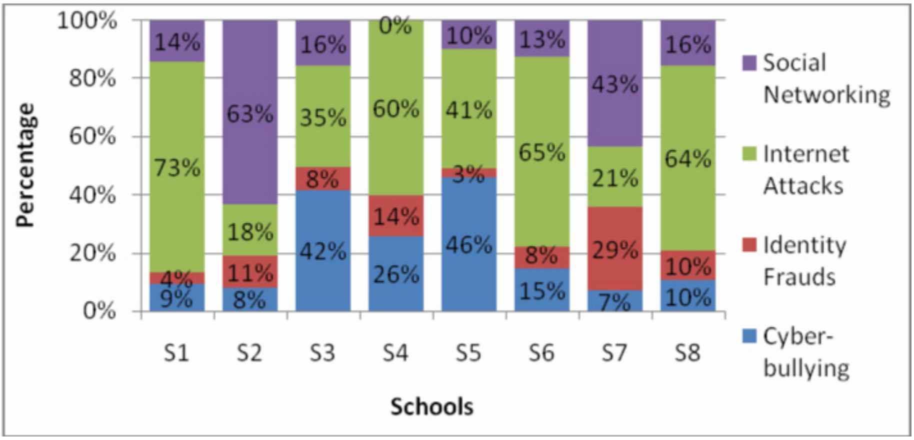

Figure 3: Ranking of Risks

In half of the schools, the participants felt that Internet attacks were the most likely risk to occur to them. However in the other schools, two sets of participants ranked social networking threats as most likely, and two ranked Cyberbullying as most likely.

Many of the participants identified that Internet Attacks were the most likely threat to affect them, with Social networking problems and Cyberbullying following. Threats arising from predatory behaviour were mentioned in the context of Social networking problems. Each discussion group identified contact from either “perverts” or “paedos” as being of concern, yet these did not score very highly when asked to rank the likelihood of occurrence to them. Concerns about giving out personal information and the problems surrounding keeping profiles private were deemed to be more likely.

The participants were asked to consider “who protects you?” and the responses fell into four main categories with people at the top:

Category	%
People	41
Software	38
Organisations	20
Hardware	1

Table 1: Percentage of responses for Who Protects you?

Of interest here is the spread of perceptions. In four of the schools participants suggested that software was the most prevalent form of protection, which included firewalls, filtering and anti-virus. Two groups put people ahead of software.

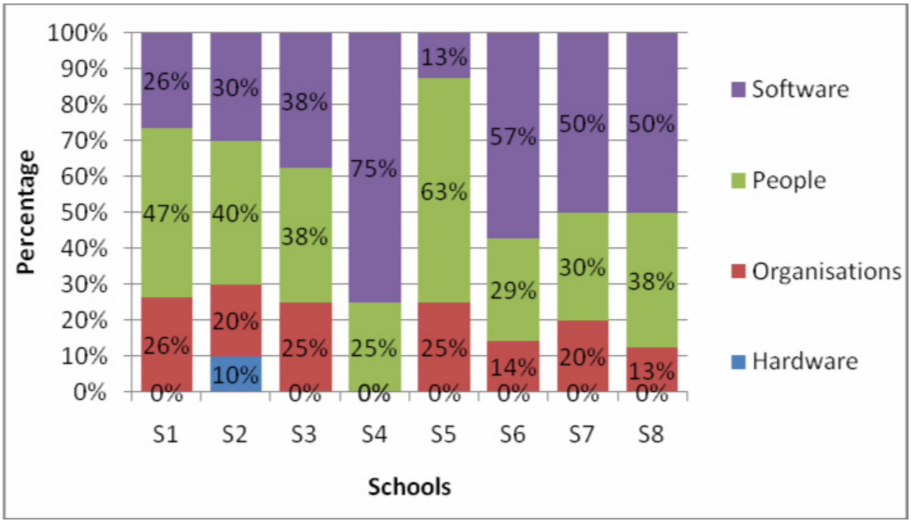

Figure 4: Who protects you?

5. Discussions

The results revealed that young people were aware of the key issues surrounding online safety and security. During the discussion groups they were able to describe clearly the types of threats that existed along with a realistic idea of the likelihood of occurrence of those threats in their own lives. They were also able to articulate a range of protection mechanisms that they might make use of which were balanced between the use of software and the actions of authoritative individuals.

Throughout the discussions it was evident that young people were able to acknowledge the threats and risks that could be found in the online environment, but as would be expected, it did not stop them from participating fully in using those technologies. The class lists were used as a way of cross-referencing the actions of the participants with their articulation of the risks and it became clear that they did not deem the risks to be relevant to them. Only when faced with the evidence did they accept that their actions might need to change, and indeed later in the project it was found that they did.

Another interesting comparison to make was that of the school that had recently had Internet Safety sessions delivered by the local children's services did not identify any more risks than those schools that had not had the sessions, but their behaviour demonstrated a difference.

6. Conclusions

This paper has demonstrated that risk culture may well be influencing the *delivery* of the awareness raising initiatives, but it has no place in influencing the *activities* of the young people at whom the messages are directed. Direct intervention by projects such as the peer-education project can be seen as having more of an effect.

The awareness raising activities need to have a balanced approach, so that they give enough information so that individuals are informed and to be able to make informed decisions. The messages should be relevant to the people they are delivered to. There is also room for activities and actions that will directly influence individuals' behaviour and as yet, the awareness activities in terms of keeping children safe online have not yet achieved that goal.

7. References

Bate, R (2000) Life's Adventure: Virtual Risk in a Real World, Butterworth-Heinemann, Oxford.

Bauwens, J., Lobe, B. and Tsakiki, L. (2008), Researching online risks and opportunities across Europe. EU Kids Online. www.lse.ac.uk/collections/EUKidsOnline/SegersaBauwensCopenhagen17.10.08.ppt. Accessed 29th April 2009.

Becta, (2006), Safeguarding children in a digital world: Developing a strategic approach to e-safety.

Bennett, (2007) Children who have everything, except the freedom to play outside. The Times Online. http://women.timesonline.co.uk/tol/life_and_style/women/families/article1884426.ece Accessed 29th April 2009

Brook, S, (2009), , Guardian online. http://www.guardian.co.uk/media/2009/apr/28/daily-express-peter-hill-mps. Accessed 29th April 2009

Byron, T (2007) Safer Children in a Digital World. London: UK Government.

CEOP, (2007), ThinkUKnow, http://www.thinkuknow.co.uk/. Accessed 29th April 2009.

CEOP, (2007a) Child Exploitation and Online Protection Centre, www.ceop.gov.uk. Accessed 29th April 2009.

Chat Danger, (2004), Chat Danger, http://www.chatdanger.com/chat/, accessed 29th April 2009.

Childnet International, (2004), ChildNet International, http://www.childnet-int.org/, accessed 29th April 2009.

DFCSF, (2008), Government Launches New UK Council for Child Internet Safety, Department for Children, Schools and Families, 28th September 2008, http://www.dcsf.gov.uk/pns/DisplayPN.cgi?pn_id=2008_0215 Accessed 29th April 2009

Europa, (2009), Social Networking: Commission brokers agreement among major web companies, http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0209/social_networking.htm. Accessed 29th April, 2009.

Fleming, M.J., Greentree, S., Cocotti-Muller, D., Elias, K.A., Morrison S., (2006) Safety in Cyberspace: Adolescents safety and exposure online. Youth and Society. 2006. Vol. 38. No. 2. P135. Sage.

Furedi, F (2002) Paranoid Parenting. Chicago: Chicago Review Press Inc.

Gerrard, N (2004) Soham: A Story of our Times. Short Books, London.

Hillingdon, (2009), E-Safety Sub-group, http://www.hillingdon.gov.uk/index.jsp?articleid=16275. Accessed 29th April 2009

Insafe Foundation, (2009), European Network of E-Safety Awareness Nodes, www.saferinternet.org. Accessed 29th April 2009

Kennedy, T. L.M. Smith, A, Wells, A.T & Wellman, B (2008) Networked Families. October 2008. www.pewinternet.org/PDF/r/266/report_display.asp Accessed 29th April 2009

LaRose, R., Rifon, N.J., Enbody, R., (2008) Promoting personal responsibility for Internet Safety. Communications of the ACM. March 2008. Vol 51. No. 3.

Panorama, (2008) One click from capture, http://news.bbc.co.uk/1/hi/programmes/panorama/7416621.stm. Accessed 29th April 2009

Pilcher, J and Wagg, S, (1996) Thatcher's children?: politics, childhood and society in the 1980s and 1990s, Routledge, London.

Sharples, M, Graber, R, Harrison, C, & Logan, K (2008) E-Safety and Web 2.0. Research Report, Becta.

Sorted, (2006), Sorted, ChildNet International, http://www.childnet-int.org/sorted/ Accessed 29th April 2009.

Staksrud, E, Livingstone, S, & Haddon, L (2007) What Do We Know About Children's Use of Online Technologies? EC Safer Internet Plus Programme, London: EU Kids Online.

Tynes, B.M., (2007) Internet Safety Gone Wild? Sacrificing the Educational and Psychosocial Benefits of Online Social Environments. Journal of Adolescent Research. Vol. 22. No. 6. November 2007