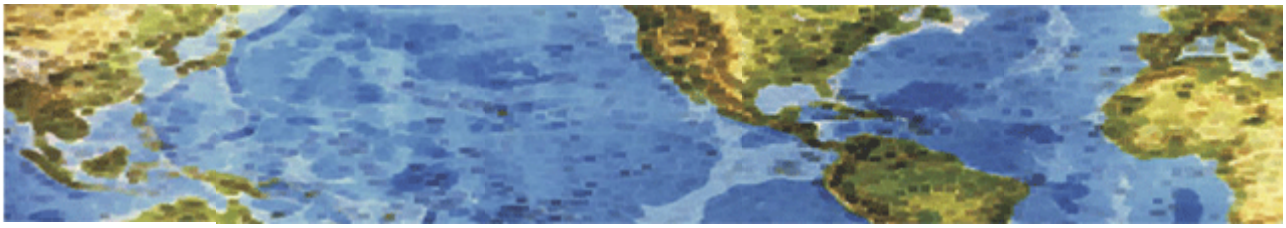
HALL ASSOCIATES



Risk-Based Decision Making Commentary
31 March 2014 Newsletter

Google Glass Partnership: What It Means For Privacy and Security

Google Glass announced last week that it is joining forces with eyewear giant Luxottica (the makers of Ray-Ban and Oakley) to **design, develop, and distribute "innovative iconic wearable devices**". Google Glass (for those of you not keeping up on new technology) is essentially **a hands-free smartphone**, offering users the ability to take pictures, surf the web, and check the weather all with Glass' minimalistic touchpad. When introduced last year, it raised obvious privacy concerns.

Google is not the only company innovating their technology in a way that deteriorates privacy – Facebook recently announced their DeepFace facial recognition software can match faces with near human accuracy. Facebook can say with 97.25% accuracy whether a photo contains a specific face. Humans can perform the same task with 97.53% accuracy.

The combination of the two has the ability to create a rather dire privacy situation. If Google Glass technology is implemented on normal, everyday glasses, people will be able to snap silent pictures of you (or anything else) without your knowledge. The snapshots can then be uploaded to Facebook where DeepFace identifies you with better accuracy than a human. Seamlessly. Do we now have to start checking for wearable devices and require glasses to be left outside of meetings like cellphones? Do you have a policy that covers anyone wearing a "smartphone" (with all its recording capabilities and connected to the internet) in your facility, in your meetings, around your information?

Pushing forward with these technologies might ultimately help our online and offline privacy. Why? **Because we value our privacy.** In the past, having privacy has been sort of like breathing: we've always taken it for granted. **This is no longer true.** As companies continue to violate our privacy on and offline, people may actually fight back with more gusto than ever before. Many people have already deserted the conventional, convenient ways they once knew in favor of a more private online experience. Stats don't lie: the private search engine, DuckDuckGo, more than doubled its search queries in 2013 and ad-blocking tools are now the most popular browser extension on the web.

Clearly, people value their online (and offline) privacy and will seek out tools to protect their personal, private information - especially when it can be accessed and used without their permission in the real world. Google Glass pushes the privacy envelope; that's for sure. So are we becoming literally one with technology? And how will we change to accommodate these things?

http://www.abine.com/blog/2014/google-glass-privacy-concerns/

HALL ASSOCIATES

Cyber-Security To Be Taught In UK Schools

Yesterday´s breaking news revealed that plans to teach children as young as 11 about careers in cyber-security was announced by the Department for Business, Innovation and Skills. This announcement **highlights the current cyber-skills shortage in the UK and the growing need for technical skills to combat the evolving cyber threat, and foster long-term economic growth.**

From this news, Thales UK & McAfee have made the following comments:
Peter Armstrong, director of cyber security, Thales UK - This new report highlights the positive and necessary steps that are needed to tackle the UK's cyber skills gap. This incentive to push cyber-security education into schools should be welcomed by the security industry and government. Any initiative that aims to increase the general capability and awareness in the cyber defense space and ultimately strengthen the UK's overall cyber defense posture, should be implemented as soon as possible to continually address the evolving cyber threat we face. It is important that schools are able to start supporting organizations by training up the next generation of cyber security experts from a young age, giving them the necessary tools and skills to deal with the latest cyber threats in the workplace.

Graeme Stewart, director of public sector strategy and relations, McAfee - The government certainly needs to be behind educating the next generation in schools across the country to address the real and imminent threat the cyber-skills shortage poses. In addition with the Government driving its own digital transformation agenda, and cyber security being reclassified to a tier-one national security threat, never has there been more pressure for the public sector to prove it is rectifying this skills gap.

Put simply, the UK has not provided the right standards of ICT education for young people over the last 20 years and it is clear the ICT curriculum has not kept pace with developments. The end result is a generation of young adults who are comfortable consuming ICT, yet do not understand nor appreciate the importance of building security into the design. Steps are now being taken to rectify these issues, but ultimately we are still facing a gap of about 15 years where there will be a significant skills crisis.

Interesting. At least the UK is trying to address teaching needed skills for the cyber age. Should our schools add this to their curriculums? Certainly our kids are using the latest technologies without much in the way of education about the threats and vulnerabilities inherent in those gadgets and devices. This also applies to our personnel and ourselves, in most cases. Education and knowledge is our only power in cyberspace and we have precious little of either.
http://www.informationsecuritybuzz.com/cyber-security-taught-schools/