A call for International Collaboration and Funding in the Fight Against CyberCrime

The International Cyber Security Protection Alliance (ICSPA) (the global, business-led, not-for-profit Alliance) is calling on governments interested in providing a more safe and secure cyber future for their citizens and business communities, to fund programmes, projects and activities that will seek to ensure that their Internet users are "cyberfit" to meet the constantly evolving challenges brought about by the inexorable growth in online criminality.

Business led the way by establishing the ICSPA in July 2011; its Chief Executive, John Lyons, makes the case in this article, for international financial support from governments, in order to accelerate the execution of its mission – to reduce the harm from cyber criminality globally, by working with governments, law enforcement agencies and businesses to provide sustainable solutions in the fight against cyber crime.

Fighting CyberCrime Together

39 countries from the EU and elsewhere have either ratified or acceded to the Budapest Convention on Cybercrime. Many more governments around the world understand the significant economic and societal benefits that the Internet delivers to their citizens and businesses. Equally, these same governments recognise the absolute priority they must give to fighting cyber crime and to developing strong cyber defences.

My contention is that by acting collaboratively to fund programmes of work to deliver benefits back to citizens and to help small and medium sized business communities better defend themselves against cyber threats, will, I believe, provide the boost that economies desperately need to help break out of this decade of austerity.

The return on investment to governments that decide to resource these programmes of work would be measurable and sustainable. Citizens would benefit directly and small businesses, the bed-rock of many national economies, would be better able to protect their intellectual property and promote the creation of new business opportunities and jobs.

Imagine what we could achieve together, if 39 countries, each donated 1 million Euros per annum for the next 5 years to a collaborative fight against cyber crime? Directing funding that would be used to carry out programmes of activities designed specifically to deliver benefits to citizens and small businesses, thus generating savings far in excess of these amounts by reducing the opportunity for cyber criminality.

If nations really care about making a step-change in the ability of Internet users to become more safe and secure online, they should act now and support this initiative. An initiative that will help citizens understand what they need to do to become more secure – whilst learning to accept some personal responsibility for securing their home networks and devices. These programmes of work are not just about raising awareness – although education and training are vitally important to us all. The projects will be extensive in their scope and reach, but all designed with one purpose – to reduce the harm from cyber crime to our most vulnerable citizens and business communities.

Getting "CyberFit for 2020" – is an international imperative which governments can no longer ignore.

By collaborating and by sharing information, knowledge and good practice, donor governments, law enforcement agencies, businesses and academia can work together within an expanded ICSPA community to ensure that public funds will be put to agreed projects that will deliver tangible results right back to those nations who have supported the programme.

Getting CyberFit for 2020

Examples of CyberFit Projects which could be deployed nationally across many nations in many languages, which have passed the ICSPA concept stage and are ready for development, are as follows:

- **Cyber Awareness Apps** for adults and cyber games for children and young people. The cyber apps are designed to alert users to new threats and scams and to help them clean-up their devices. The games for children will provide games in a range of formats designed to be fun and engaging whilst teaching our most vulnerable citizens how they can stay safe online. By the time they progress through these games and start to use the adult apps they will be "cyberfit" for adulthood.
- **CyberBridge** – a collaborative business case between the ICSPA and the City of London Police in England – designed to clean-up the estimated 5.5 million infected IP addresses in the UK – mostly in the hands of domestic broadband users. These mainly Trojan-infected devices are causing significant financial losses to online retailers and banks.
- **CyberFit for Business** – a series of awareness, educational and training packages designed for small and medium sized business communities to ensure that they are optimising their cyber defences. Assistance programmes include online training modules, cyber assistance call centres and visits by properly qualified and certified Internet Security specialists to provide direct support if required.
- **CyberFit for Citizens** – awareness, education and training programmes together with marketing and communications activities designed to help citizens understand online threats and scams and to give them the training and tools to ensure that they can help themselves

become more safe and secure online. The thrust of these programmes would be to ensure that citizens understand the great value the Internet delivers whilst helping them accept that they must take some personal responsibility for being "good cyber citizens".

- **GetSafeOnline** – an existing educational resource for citizens in the UK, with similar websites and resources in other countries, that could be harmonised and adapted to suit local languages and cultures throughout supporting nations.
- **Project Aurora** – designed to provide consultancy to countries that require a cyber health check and audit of their existing programmes and infrastructures. Designed to result in a fully costed project plan and business case which would provide governments with a road map to a more cyber resilient future.
- **Cyber Crime Impact Studies** – conducted already in Canada and designed to provide governments with an independent assessment of the scope and nature of cyber crime targeted against its business communities. The results are used to help policy makers in government and to support law enforcement and business communities decide where best to channel hard-earned resource.
- **Establishing ICSPA business hubs** internationally – designed to create public /private sector engagement for local and national projects to fight cyber crime. Each donating country would be provided with an ICSPA presence to coordinate the programmes and projects that were being undertaken and to liaise with stakeholders to ensure successful execution of national programmes of work.

Clearly, there will be other projects that will come to fruition, but focus is imperative and the harnessing of global expertise to provide best of breed solutions that work, is where our energies should be deployed.

The Rationale for this new ICSPA Initiative

Getting CyberFit for 2020 is an independent ICSPA initiative aimed at delivering value to citizens and business communities. It is void of politics and inspired by the recognition over many years that together we must implement cyber programmes that will help our citizens become more productive online and when using their mobile devices, whilst ensuring that they remain safe and secure whilst doing so.

No one government can take the lead on this. Yes leadership is essential but nations that need help do not want it thrust upon them by another nation that, perhaps, thinks it has all the answers.

Everyone knows that we need to work collaboratively to fight this global phenomenon – world leaders know that, business leaders do it every day and citizens simply marvel at the speed with which they can be compromised online whilst carrying out the most fundamental tasks.

Some nations report falling crime figures - yet we all know that the criminals haven't packed up and gone home. The truth is that very well organised criminal groups are now concentrating and directing their exploits and activities at a much wider audience – reaching millions of citizens online at the touch of a keyboard. Making millions of dollars a week without much prospect of getting caught, and when they do, spending very little time behind bars. But let's be honest - there will never be enough law enforcement officers in the world to investigate and lock-up all online criminals. We as citizens need to recognise that and governments need to be truthful about it.

Internet criminality funds real, physical harm to families and children

The final argument in favour of establishing this government funded work is that there exists a more sinister outcome to this continued growth in cyber criminality. Whilst citizens are generally reimbursed for their losses by online retailers and banks, who want to avoid adverse publicity – the funds and proceeds of crime amassed by criminal groups are re-invested by them to create real, physical harm in our societies. Online proceeds are used to fund people trafficking, gun crime, illegal drug smuggling, paedophilia and, yes, to fund terrorist planning and operations.

Creativity is required to change attitude and behaviour

So long as citizens fail to recognise the link between their (temporary) financial loss and harmful criminal activity downstream – they will continue not to care about their personal cyber hygiene. Because it's not hurting them personally, they will continue to ignore messages which implore them to be more diligent about their online safety and security.

Communications programmes designed to bring about the changes we need in citizens attitude and behaviour will need the very best creative talents that exist in order to make the impact that we all need and desire. Harmonising these programmes across many nations, reaching out to all cultures and faiths, recognising the powerful effect that great brands have on our people and their children, is just the sort of thinking that we will need to harness if we are to succeed in becoming CyberFit for 2020.

John Lyons is Chief Executive of The International Cyber Security Protection Alliance (ICSPA) and can be contacted on john.lyons@icspa.org

Notes to Editors:

About the ICSPA

The ICSPA is a business-backed, not-for-profit, global organisation that provides assistance to countries and their law enforcement agencies to fight cybercrime. Its Chair is the Rt Hon David Blunkett MP, one of the UK's most dedicated politicians, who held senior Cabinet positions in Tony Blair's Labour Government.

The Alliance is supported by its business members and partners - among them some of the world's top cyber security companies, including logistics companies, retailers, payment companies and fraud prevention specialists. The ICSPA's Steering Group comprises senior business leaders from its Enterprise Member companies including Atos, Lockheed Martin, McAfee, Symantec, Trend Micro and Visa Europe.

ICSPA Partners

In Europe, the ICSPA is partnered with Europol and the European Cyber Crime Centre (EC3) and the City of London Police and has professional associations with the Global Prosecutors E-crime Network, the International Association of Prosecutors and $(ISC)^2$ – which brings together more than 86,000 information security specialists.

The ICSPA is working with governments in the Americas, Europe, Africa and Asia to help ensure business engagement in the global response to fighting cyber criminality. In the summer of 2012, the Alliance launched Project 2020, a global study of emerging cyber threats undertaken in conjunction with Europol, and their recently established European Cybercrime Centre (EC3).

For more information visit www.icspa.org

For press inquiries and requests for interviews with ICSPA, please email icspa@arpartners.com or contact:

Tim Weber: +44 20 3047 2487 or
Rishi Bhattacharya: +44 20 3047 2361