John Lyons - Launching the ICSPA – 5th July at 1430

Ladies and gentlemen, thank you all very much indeed for attending the launch of the International Cyber Security Protection Alliance. My name is John Lyons and I am the Chief Executive of the ICSPA.

This is our first opportunity to present publicly this new organisation and we are delighted that so many of you have decided to join us. I would also like to thank James Brokenshire, Home Office Minister with responsibility for Crime and Security, for making room in his busy Parliamentary schedule to speak on behalf of the Government - and to our Chairman, David Blunkett, for his guidance and huge support in helping us to get the organisation to the point where we are ready to start work in earnest. We will be hearing from James and from David in a short while.

In this room today, we also have the founding members of the ICSPA – nationally and internationally recognised and respected enterprises that have many millions of customers – business customers, government customers and consumers. They are servicing these customers in practically every country in the world, carrying out billions of transactions each year, using the Internet. So who would know better about the impact of cybercrime on business than the people in this room from our Member companies who engage in the fight against online criminality every minute of every day.

The International Cyber Security Protection Alliance is very privileged to have as our founding business members:

McAfee – Cassidian Systems (an EADS company) - Trend Micro – Shop Direct Group – Transactis – Core Security Technologies – Yodel – and most recently – Visa Europe (having so recently joined us, that the print material you see today was produced before we received their logo).

So who are we? - Why have we come together as an organisation?

What makes us different? - and what do we intend to do?

The ICSPA is a business-led, international, not-for-profit organisation formed to lead and coordinate a new global approach to combating the aggressive growth in cybercrime. We will do this by channelling funding, expertise, information-sharing about good practice and technical assistance directly to law enforcement cyber crime units in both domestic and international markets – but particularly to cybercrime agencies in countries that face the greatest challenges . To ensure that we gain maximum impact, we will also seek resource and support from the EU and from Governments and institutions that understand the need to assist countries - and that wish to join us in helping to reduce the harm caused to businesses, their customers and citizens around the world.

It is by helping to improve the capability and capacity of these law enforcement units that we expect to see a long term and sustainable effect on the inexorable growth in cyber crime.

At the same time that many governments and businesses are doing all that THEY can to secure their networks, websites and communications against cyber attack - law enforcement cyber crime units all over the world are struggling to meet the demands placed upon them by technically sophisticated adversaries. Most countries are often the unwitting and unwilling hosts to the unprecedented levels of cybercrime that we are witnessing. Businesses, their supply chains, their customers and citizens are being attacked ruthlessly and relentlessly – but the truth is, that many national law enforcement cyber crime units around the world do not have sufficient capacity or capability to handle the volume of cyber crime which we are experiencing.

We have established the International Cyber Security Protection Alliance because we realise that internationally, a number of events are combining to create a perfect storm in cyber space:

- We are all beginning to feel the strain from the implementation of global financial austerity measures – these measures are having an effect on the public funding of law enforcement agencies around the world. The people who run these agencies will inevitably be forced to tackle their highest crime priorities likely to be in the areas of violence, gun crime, drug running, counter terrorism and people trafficking. Niche areas such as cyber crime, network security investigations and digital forensics capability are, as a consequence, likely to suffer from a reduction in public funding and investment.
- At the same time, we have been witnessing recently an unprecedented growth in cyber criminality in all its guises - targeted at governments, critical national infrastructures, at businesses and at consumers. The enemy - identified as a mix of state-sponsored actors, organised criminal groups, so-called loosely organised hactavist networks and technically sophisticated individuals and terrorist groups – are running wild on the Internet, successfully engineering highly sophisticated malicious code and methodologies for delivering their payload - and with very little prospect of facing justice.
- Finally, given this scenario – public funding that might be available to counter cyber crime, will largely be channelled towards the protection of countries' critical national infrastructures – leaving commercial businesses and their customers on the receiving end of growing amounts of cyber pain. The UK is in the very fortunate position that the Government has recognised the threat that we face and has injected new funding into cyber security measures to help better protect our critical national infrastructures. The government has also supported the work of the Police Central e-Crime Unit and the Serious Organised Crime Agency by allocating much needed additional funding over the next four years. The US Government too, is taking unparalleled steps to respond to the challenges that they face from cyber attack. Alas, this is not the story that you will find if you look carefully at many other countries

whose cyber crime and security posture are not well developed. It is in the cyber crime units of these countries that the ICSPA will be able to help most.

However, even in countries like the UK, US, Canada and Australia - we must not be complacent or rest on our laurels – help will be needed here too – above and beyond that which can be provided purely from public funds.

To give you a feel for what some very capable and well-established law enforcement agencies face, let me share with you results from the US Department of Justice, Inspector General's Audit Report of April this year:

The auditors had conducted field work at the FBI Headquarters in Washington DC and at 10 of the 56 FBI field offices in various US States. They found that 36 percent of FBI Agents interviewed, reported that they "lacked the networking and counter intelligence expertise to investigate national security [cyber] intrusion cases." The auditors "also found that the forensic and analytical capability in the field offices was inadequate to support national security intrusion investigations. Some field agents believed this affected the FBI's ability to determine those responsible for intrusions."

And so, faced with the reality of the global cyber threat, diminishing public funds and law enforcement organisations with varying degrees of capability in combating cyber crime - we felt that a business-led approach, supporting a not-for-profit, independent organisation focused directly on assisting carefully selected law enforcement cyber crime units in countries that need help most – would provide a uniquely new initiative that could offer a truly collaborative and very powerful answer to the growing menace in cyber space.

So what precisely will we be doing to assist these cyber crime units?

We will be working to help fund additional cyber training for officers; we will seek to work with training organisations and academia to introduce standardised accreditation for officers – something that does not exist today. We will work to help establish information sharing mechanisms between businesses and law enforcement agencies - and by sharing the expertise of our Member companies with cyber crime units, we will seek to convey good practice across business and law enforcement organisations thus enabling more effective use of law enforcement resources. Finally, we will work together - industry, government and law enforcement to look at ways in which we can design-out vulnerabilities in new products, networks and services - aimed at making life as difficult as possible for cyber criminals, whilst engineering systems that the public can use with greater assurance of safety and security – making ease of use a priority whilst providing solutions that do not require an in-depth knowledge of computers to ensure successful and safe interaction on the Internet.

We know that we have taken on a very ambitious mission. And we don't pretend to have all the answers. So our aim is to collaborate also with already established groups that can complement our efforts and help us to achieve our aims with timely effectiveness.

I would like to finish this introduction by saying that we have been hugely encouraged and heartened by the response we have had from our founding business Members who you see here this afternoon – and from law enforcement agencies – you will hear more about our plans for working within the EU from the Minister – and delighted too by the encouragement we have received from the Governments of the US, Australia and especially the unequivocal support we have had from the UK Government.

Before I ask James Brokenshire to speak on behalf of the Government, I would like you to hear a few words of encouraging support from his boss:

PLAY THE PM'S VIDEO

I would now like to ask James Brokenshire, Home Office Minister for Crime & Security to speak on behalf of the Government. Ladies and gentlemen, James Brokenshire -