CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org
Charity Registration Number: 208223

Transcript

Cyber Security Information Sharing Programme

The Rt. Hon. Francis Maude MP

27 March 2013

Francis Maude:

I think we can all agree, we ignore the cyber threat at our peril.

This applies to government and industry equally. 93% of large corporations and three quarters of small businesses are estimated to have had a cyber security breach in the past year. While government blocks on average over 33,000 malicious emails, every month.

A successful attack has huge consequences. We know of one company that lost 100GB of data in single incident; that's roughly a 20 million page Word document.

Last year a 9-day attack by the hacker group Anonymous caused Paypal to lose more than £3.5 million.

And the threat is accelerating.

I spoke on cyber security in December - since then there have been more high-profile attacks.

Just over a week ago computer networks running three major South Korean banks and the country's two largest broadcasters were paralyzed in cyber-attacks. And last month the New York Times told how they came under a four-month long assault from attackers breaking into their computers and mining their databases.

Cyber security is unsurprisingly topping the policy agenda. President Barack Obama recently set out a new plan to protect the United States' critical infrastructure against cyberattacks –

And last month the EU proposed cybercrime reporting rules as part of its new Cyber Security Strategy, which we will need to consider carefully in the UK.

This is a fast-paced, high stakes, global battleground. And here in the UK our responses have to be fast and flexible – we cannot afford to be on the back foot.

Because there is – I don't need to remind you – a lot at stake here. The web is vital for our way of life, vital for our economy. The UK's Internet ecosystem is now worth £82 billion a year - and this is set to rise.

And we are here today because we are all invested in the success of the internet. And if we want to go on enjoying the benefits of cyberspace – we need to team up to fight our common enemies.

That is what this new Cyber Security Information Sharing Partnership (CISP) is all about: Government and industry working together to build a

comprehensive picture of the cyber threat and coming up with the best defences.

I know industry played a crucial role in designing this partnership so it would work for you – and I'm delighted so many companies are signed up to it. Now, we have to make it work – and that will hinge on each of you continuing to play an active role.

The Government is committed to playing its part –

We have already committed £650million to the transformative National Cyber Security Programme to bolster the UK's cyber defences.

And just over a year ago I published a cross-government Cyber Security Strategy, which set out how we would build a more trusted and resilient cyberspace. In December I published a report setting out our significant progress against the strategy's key objectives.

But – we know there is a long way to go. And we can't fight this battle alone. The private sector is the largest economic victim of cyber crime – and is the most important line of defence against cyber criminals.

In this last year we have worked very closely with industry to improve our understanding of the threat – and raise awareness.

For example we have launched a 'Cyber Security Guidance for Business' document for industry Chief Executives, which sets out how board members and senior executives should safeguard their most valuable assets, such as personal data, online services and intellectual property.

This is important: Sir Iain Lobban, the GCHQ Director, estimates 80% of attacks could be thwarted by basic security measures such as updating software.

We are also working closely with the private sector and standards bodies to support the development of industry-led 'organisational standards', to ensure there is clarity about what good practice looks like for an organisation trying to manage its cyber risk.

This will not only give firms clear steps to follow in managing their cyber risk – it will also give customers and investors a clear indicator of whether a firm is taking this risk seriously.

We shouldn't forget that cyber security also presents an opportunity for companies with the growth in demand in the UK and globally, for vibrant and innovative cyber security services.

Last week the first meeting of the cyber growth partnership was held where businesses and Government came together to agree how best to support the growth of the UK cyber industry by boosting sales both domestically and overseas.

We are in a stronger position as a result of these efforts – but there is no room for complacency.

It is abundantly clear to anyone working in cyber security that no-one has anything like complete visibility of the problem. Cyberspace is simply too vast for any organisation – public or private sector – to have sight on everything that's going on.

But we know getting the best picture possible is key to us keeping one step ahead of the threat.

We started to tackle this issue two years ago when the Prime Minister held an event at Number 10 for business senior executives, to underline the benefits of a real and meaningful partnership between industry and government.

The government's proposal was this: by building a community of public and private partners, we could all pool our information on cyber threats and increase our visibility of cyber threats for mutual benefit.

The result was a pilot, Project Auburn, to explore how industry and government could share information on current threats and strategies - this also included information from the intelligence services.

Around 80 companies from many different sectors signed up this pilot, and I know many of you are represented here today.

The pilot generated some notable success stories, with firms in different industry sectors sharing important information. For example a firm detecting reconnaissance activity against its network was able to share details of that nascent attack with its peers, who were then able to protect themselves from the threat before it caused damage.

As a result we kept the scheme going - increasing the number of industry partners to around 160. This provided important support to some key sectors such as transport during the Olympics.

But there was clearly scope to take this initiative even further -

And over the last nine months industry and government have been designing a new and improved structure that would put cyber information sharing on a permanent footing –

The new Cyber Security Information Sharing Partnership we are launching today will give government and industry a far richer, more immediate intelligence picture of the cyber threat.

For the first time a new secure, virtual collaborative environment will allow government, including the Security Service, GCHQ and the National Crime Agency, and industry partners to exchange information on threats and vulnerabilities as they're identified.

A team of experts, known as the Fusion Cell and made up of analysts from industry and the law enforcement and intelligence communities, will draw together a single intelligence picture of cyber threats facing the UK for the benefit of all partners.

This will be the first time such a diverse set of skills and experience will be brought together in one location, and it will mean businesses will have access to the best strategies for preventing the sorts of attacks that cost you so much time and money.

CISP will initially remain targeted at those private sector organisations that are at greatest risk from cyber threats and are already partnered with the Centre for the Protection of National Infrastructure.

But ultimately we want to extend the benefits of this scheme as widely as possible, and we are already in the process of setting up further pilots beyond the critical national infrastructure, including with SMEs. Interested organisations can register their interest through the CISP website.

We know that CISP has real potential to add value to everyone who participates. But I can't stress enough today that this service will be very much what you make of it. There is nothing compulsory about it – it will be up to all members to share information so that others can benefit. And companies will be free to choose the level of detail they provide and how widely that information will be shared.

The more volume, the more traffic there is – the more useful it will be to all of us. The more information each member makes available to the community – the richer our collective knowledge.

Conclusion

We have come a long way since that meeting in No 10. And I'd like to take this opportunity to thank those industry partners who have volunteered resources, at their own cost, to make this initiative work.

This kind of working is the future: government and industry working hand-in-hand to fight a common threat.

Some have suggested a more regulated approach – but our experience here in the UK shows that a voluntary arrangement based on trust and shared interests can work.

There is a growing realisation that it is only by working together - not limited by the boundaries of commercial interests – that we can ensure that the UK can continue to realise the benefits of a vibrant, open and safe online environment.

This is a shared challenge and we all share a responsibility to meet it. Today's launch is another big step forward – now we need to keep the momentum building.