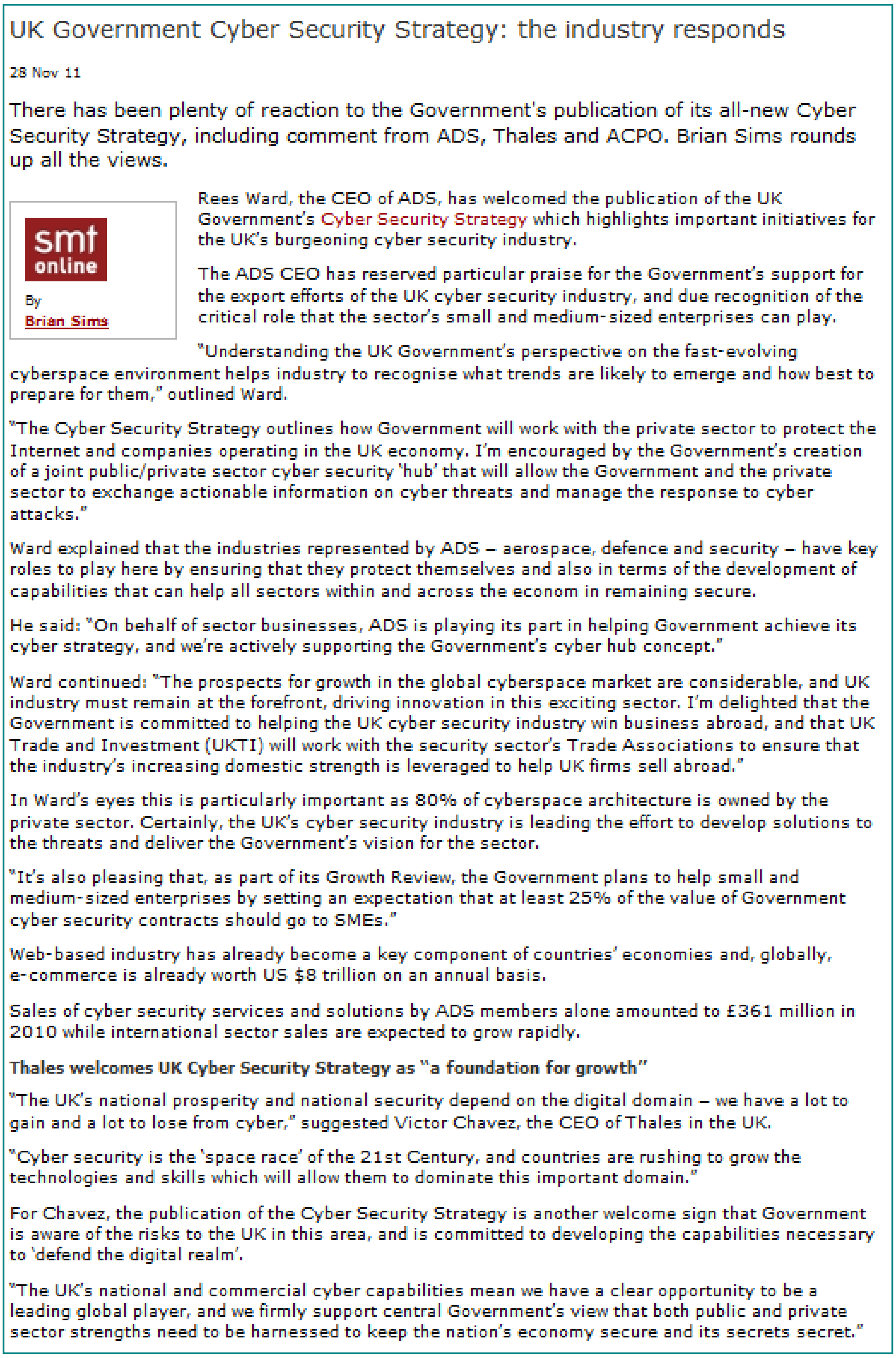
Info4 Security

28 November 2011



UK Government Cyber Security Strategy: the industry responds

28 Nov 11

There has been plenty of reaction to the Government's publication of its all-new Cyber Security Strategy, including comment from ADS, Thales and ACPO. Brian Sims rounds up all the views.

By
Brian Sims

Rees Ward, the CEO of ADS, has welcomed the publication of the UK Government's Cyber Security Strategy which highlights important initiatives for the UK's burgeoning cyber security industry.

The ADS CEO has reserved particular praise for the Government's support for the export efforts of the UK cyber security industry, and due recognition of the critical role that the sector's small and medium-sized enterprises can play.

"Understanding the UK Government's perspective on the fast-evolving cyberspace environment helps industry to recognise what trends are likely to emerge and how best to prepare for them," outlined Ward.

"The Cyber Security Strategy outlines how Government will work with the private sector to protect the Internet and companies operating in the UK economy. I'm encouraged by the Government's creation of a joint public/private sector cyber security 'hub' that will allow the Government and the private sector to exchange actionable information on cyber threats and manage the response to cyber attacks."

Ward explained that the industries represented by ADS – aerospace, defence and security – have key roles to play here by ensuring that they protect themselves and also in terms of the development of capabilities that can help all sectors within and across the econom in remaining secure.

He said: "On behalf of sector businesses, ADS is playing its part in helping Government achieve its cyber strategy, and we're actively supporting the Government's cyber hub concept."

Ward continued: "The prospects for growth in the global cyberspace market are considerable, and UK industry must remain at the forefront, driving innovation in this exciting sector. I'm delighted that the Government is committed to helping the UK cyber security industry win business abroad, and that UK Trade and Investment (UKTI) will work with the security sector's Trade Associations to ensure that the industry's increasing domestic strength is leveraged to help UK firms sell abroad."

In Ward's eyes this is particularly important as 80% of cyberspace architecture is owned by the private sector. Certainly, the UK's cyber security industry is leading the effort to develop solutions to the threats and deliver the Government's vision for the sector.

"It's also pleasing that, as part of its Growth Review, the Government plans to help small and medium-sized enterprises by setting an expectation that at least 25% of the value of Government cyber security contracts should go to SMEs."

Web-based industry has already become a key component of countries' economies and, globally, e-commerce is already worth US $8 trillion on an annual basis.

Sales of cyber security services and solutions by ADS members alone amounted to £361 million in 2010 while international sector sales are expected to grow rapidly.

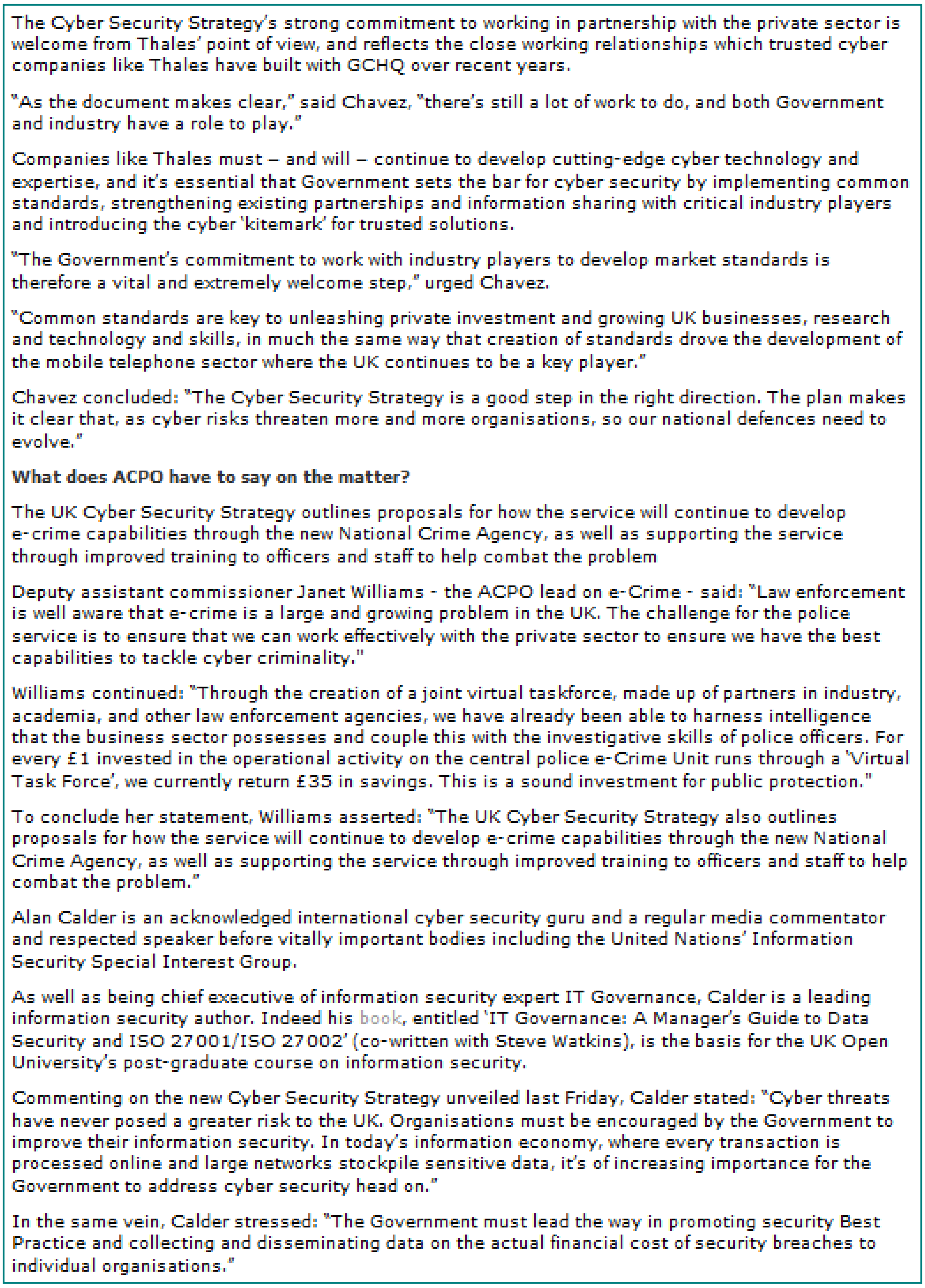
Thales welcomes UK Cyber Security Strategy as "a foundation for growth"

"The UK's national prosperity and national security depend on the digital domain – we have a lot to gain and a lot to lose from cyber," suggested Victor Chavez, the CEO of Thales in the UK.

"Cyber security is the 'space race' of the 21st Century, and countries are rushing to grow the technologies and skills which will allow them to dominate this important domain."

For Chavez, the publication of the Cyber Security Strategy is another welcome sign that Government is aware of the risks to the UK in this area, and is committed to developing the capabilities necessary to 'defend the digital realm'.

"The UK's national and commercial cyber capabilities mean we have a clear opportunity to be a leading global player, and we firmly support central Government's view that both public and private sector strengths need to be harnessed to keep the nation's economy secure and its secrets secret."



The Cyber Security Strategy's strong commitment to working in partnership with the private sector is welcome from Thales' point of view, and reflects the close working relationships which trusted cyber companies like Thales have built with GCHQ over recent years.

"As the document makes clear," said Chavez, "there's still a lot of work to do, and both Government and industry have a role to play."

Companies like Thales must – and will – continue to develop cutting-edge cyber technology and expertise, and it's essential that Government sets the bar for cyber security by implementing common standards, strengthening existing partnerships and information sharing with critical industry players and introducing the cyber 'kitemark' for trusted solutions.

"The Government's commitment to work with industry players to develop market standards is therefore a vital and extremely welcome step," urged Chavez.

"Common standards are key to unleashing private investment and growing UK businesses, research and technology and skills, in much the same way that creation of standards drove the development of the mobile telephone sector where the UK continues to be a key player."

Chavez concluded: "The Cyber Security Strategy is a good step in the right direction. The plan makes it clear that, as cyber risks threaten more and more organisations, so our national defences need to evolve."

What does ACPO have to say on the matter?

The UK Cyber Security Strategy outlines proposals for how the service will continue to develop e-crime capabilities through the new National Crime Agency, as well as supporting the service through improved training to officers and staff to help combat the problem

Deputy assistant commissioner Janet Williams - the ACPO lead on e-Crime - said: "Law enforcement is well aware that e-crime is a large and growing problem in the UK. The challenge for the police service is to ensure that we can work effectively with the private sector to ensure we have the best capabilities to tackle cyber criminality."

Williams continued: "Through the creation of a joint virtual taskforce, made up of partners in industry, academia, and other law enforcement agencies, we have already been able to harness intelligence that the business sector possesses and couple this with the investigative skills of police officers. For every £1 invested in the operational activity on the central police e-Crime Unit runs through a 'Virtual Task Force', we currently return £35 in savings. This is a sound investment for public protection."

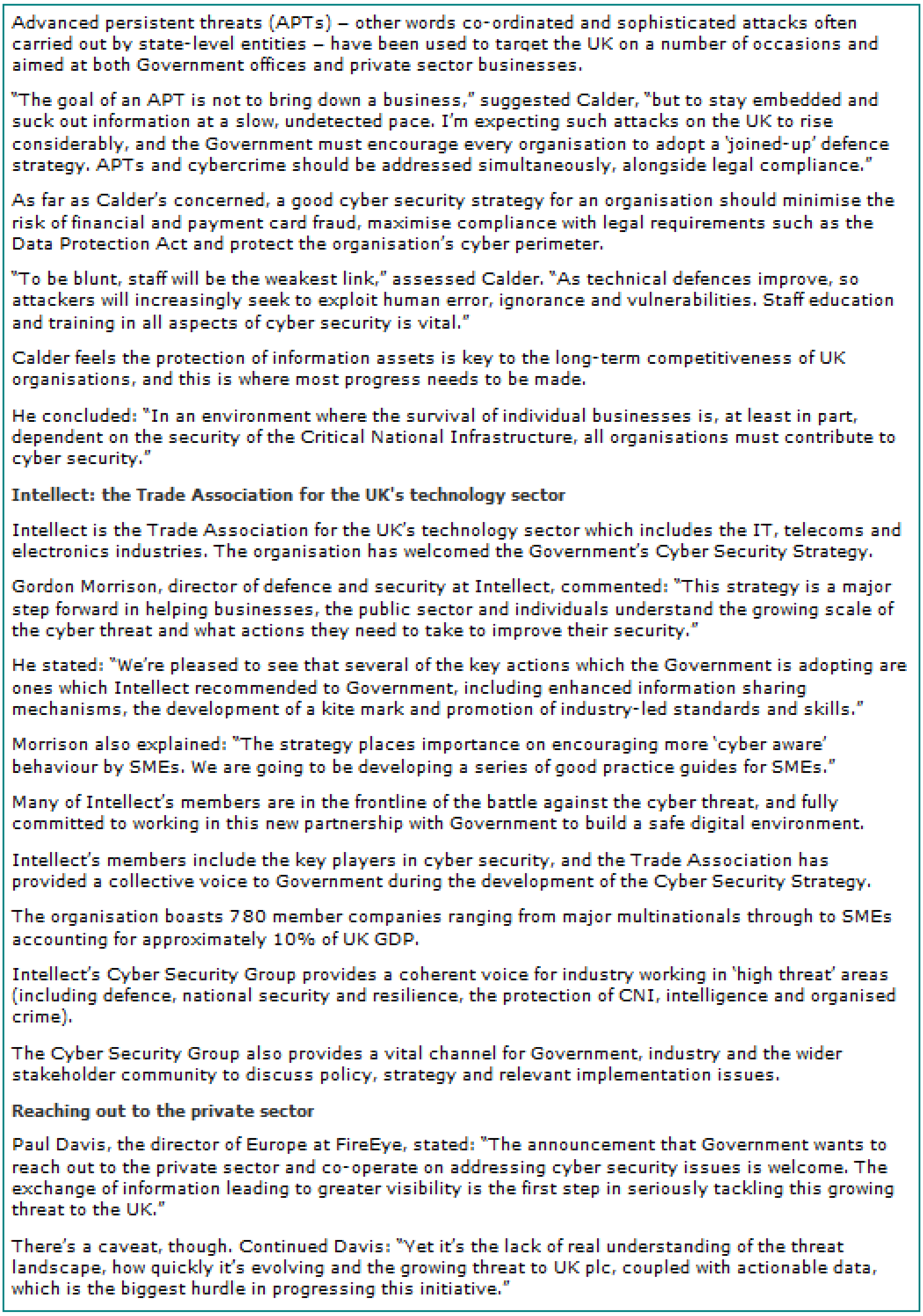
To conclude her statement, Williams asserted: "The UK Cyber Security Strategy also outlines proposals for how the service will continue to develop e-crime capabilities through the new National Crime Agency, as well as supporting the service through improved training to officers and staff to help combat the problem."

Alan Calder is an acknowledged international cyber security guru and a regular media commentator and respected speaker before vitally important bodies including the United Nations' Information Security Special Interest Group.

As well as being chief executive of information security expert IT Governance, Calder is a leading information security author. Indeed his book, entitled 'IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002' (co-written with Steve Watkins), is the basis for the UK Open University's post-graduate course on information security.

Commenting on the new Cyber Security Strategy unveiled last Friday, Calder stated: "Cyber threats have never posed a greater risk to the UK. Organisations must be encouraged by the Government to improve their information security. In today's information economy, where every transaction is processed online and large networks stockpile sensitive data, it's of increasing importance for the Government to address cyber security head on."

In the same vein, Calder stressed: "The Government must lead the way in promoting security Best Practice and collecting and disseminating data on the actual financial cost of security breaches to individual organisations."



Advanced persistent threats (APTs) – other words co-ordinated and sophisticated attacks often carried out by state-level entities – have been used to target the UK on a number of occasions and aimed at both Government offices and private sector businesses.

"The goal of an APT is not to bring down a business," suggested Calder, "but to stay embedded and suck out information at a slow, undetected pace. I'm expecting such attacks on the UK to rise considerably, and the Government must encourage every organisation to adopt a 'joined-up' defence strategy. APTs and cybercrime should be addressed simultaneously, alongside legal compliance."

As far as Calder's concerned, a good cyber security strategy for an organisation should minimise the risk of financial and payment card fraud, maximise compliance with legal requirements such as the Data Protection Act and protect the organisation's cyber perimeter.

"To be blunt, staff will be the weakest link," assessed Calder. "As technical defences improve, so attackers will increasingly seek to exploit human error, ignorance and vulnerabilities. Staff education and training in all aspects of cyber security is vital."

Calder feels the protection of information assets is key to the long-term competitiveness of UK organisations, and this is where most progress needs to be made.

He concluded: "In an environment where the survival of individual businesses is, at least in part, dependent on the security of the Critical National Infrastructure, all organisations must contribute to cyber security."

Intellect: the Trade Association for the UK's technology sector

Intellect is the Trade Association for the UK's technology sector which includes the IT, telecoms and electronics industries. The organisation has welcomed the Government's Cyber Security Strategy.

Gordon Morrison, director of defence and security at Intellect, commented: "This strategy is a major step forward in helping businesses, the public sector and individuals understand the growing scale of the cyber threat and what actions they need to take to improve their security."

He stated: "We're pleased to see that several of the key actions which the Government is adopting are ones which Intellect recommended to Government, including enhanced information sharing mechanisms, the development of a kite mark and promotion of industry-led standards and skills."

Morrison also explained: "The strategy places importance on encouraging more 'cyber aware' behaviour by SMEs. We are going to be developing a series of good practice guides for SMEs."

Many of Intellect's members are in the frontline of the battle against the cyber threat, and fully committed to working in this new partnership with Government to build a safe digital environment.

Intellect's members include the key players in cyber security, and the Trade Association has provided a collective voice to Government during the development of the Cyber Security Strategy.

The organisation boasts 780 member companies ranging from major multinationals through to SMEs accounting for approximately 10% of UK GDP.

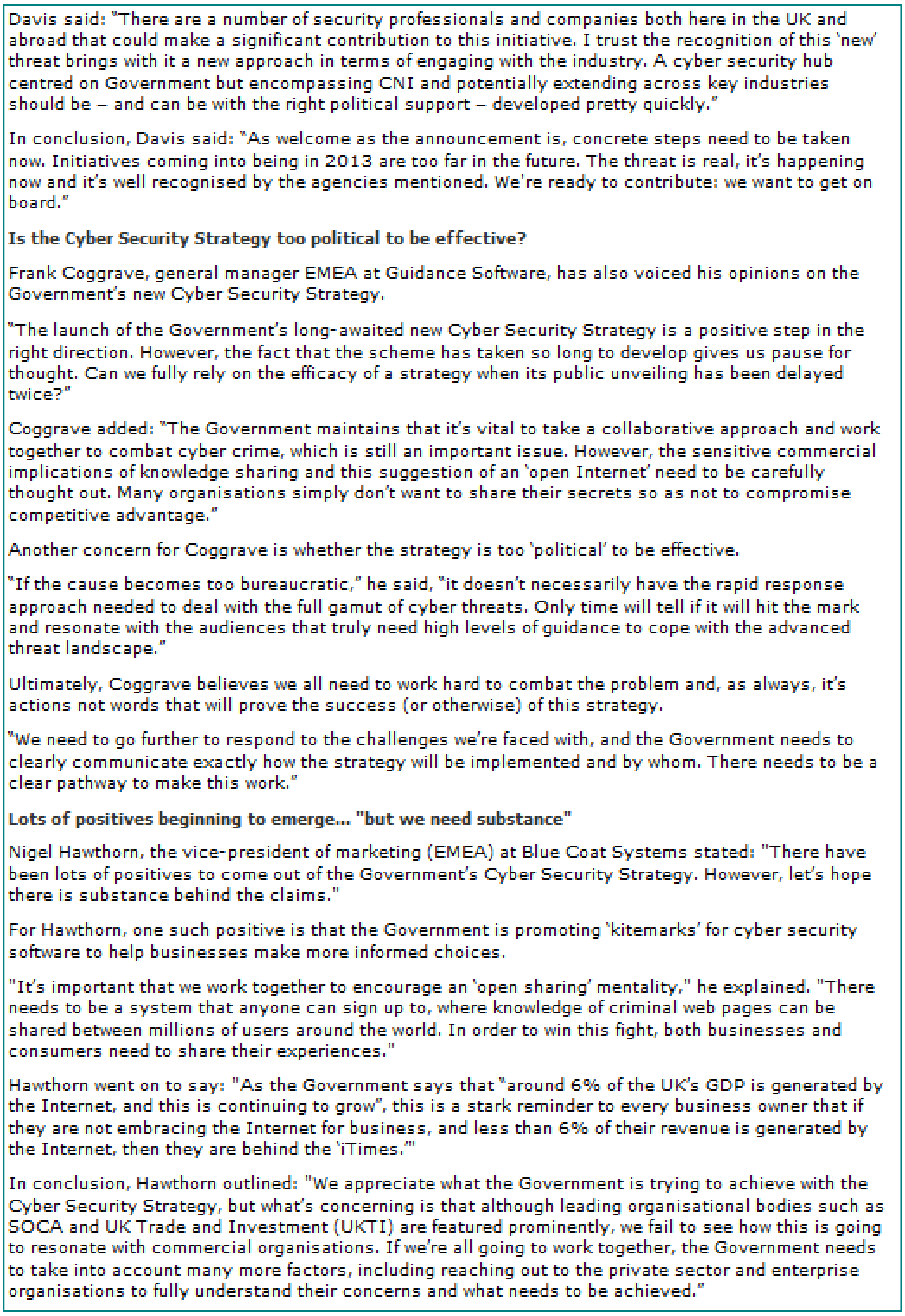
Intellect's Cyber Security Group provides a coherent voice for industry working in 'high threat' areas (including defence, national security and resilience, the protection of CNI, intelligence and organised crime).

The Cyber Security Group also provides a vital channel for Government, industry and the wider stakeholder community to discuss policy, strategy and relevant implementation issues.

Reaching out to the private sector

Paul Davis, the director of Europe at FireEye, stated: "The announcement that Government wants to reach out to the private sector and co-operate on addressing cyber security issues is welcome. The exchange of information leading to greater visibility is the first step in seriously tackling this growing threat to the UK."

There's a caveat, though. Continued Davis: "Yet it's the lack of real understanding of the threat landscape, how quickly it's evolving and the growing threat to UK plc, coupled with actionable data, which is the biggest hurdle in progressing this initiative."



Davis said: "There are a number of security professionals and companies both here in the UK and abroad that could make a significant contribution to this initiative. I trust the recognition of this 'new' threat brings with it a new approach in terms of engaging with the industry. A cyber security hub centred on Government but encompassing CNI and potentially extending across key industries should be – and can be with the right political support – developed pretty quickly."

In conclusion, Davis said: "As welcome as the announcement is, concrete steps need to be taken now. Initiatives coming into being in 2013 are too far in the future. The threat is real, it's happening now and it's well recognised by the agencies mentioned. We're ready to contribute: we want to get on board."

Is the Cyber Security Strategy too political to be effective?

Frank Coggrave, general manager EMEA at Guidance Software, has also voiced his opinions on the Government's new Cyber Security Strategy.

"The launch of the Government's long-awaited new Cyber Security Strategy is a positive step in the right direction. However, the fact that the scheme has taken so long to develop gives us pause for thought. Can we fully rely on the efficacy of a strategy when its public unveiling has been delayed twice?"

Coggrave added: "The Government maintains that it's vital to take a collaborative approach and work together to combat cyber crime, which is still an important issue. However, the sensitive commercial implications of knowledge sharing and this suggestion of an 'open Internet' need to be carefully thought out. Many organisations simply don't want to share their secrets so as not to compromise competitive advantage."

Another concern for Coggrave is whether the strategy is too 'political' to be effective.

"If the cause becomes too bureaucratic," he said, "it doesn't necessarily have the rapid response approach needed to deal with the full gamut of cyber threats. Only time will tell if it will hit the mark and resonate with the audiences that truly need high levels of guidance to cope with the advanced threat landscape."

Ultimately, Coggrave believes we all need to work hard to combat the problem and, as always, it's actions not words that will prove the success (or otherwise) of this strategy.

"We need to go further to respond to the challenges we're faced with, and the Government needs to clearly communicate exactly how the strategy will be implemented and by whom. There needs to be a clear pathway to make this work."

Lots of positives beginning to emerge... "but we need substance"

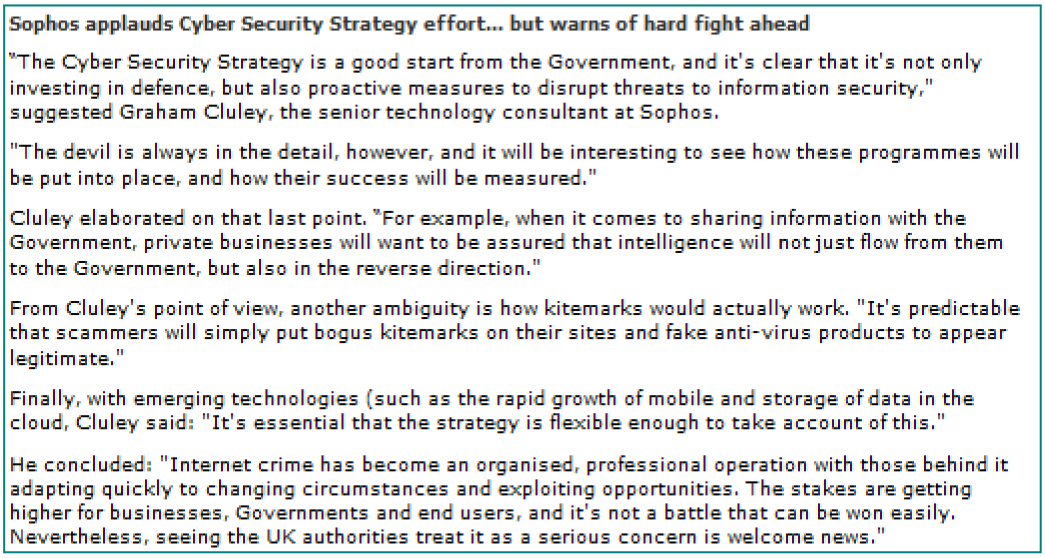
Nigel Hawthorn, the vice-president of marketing (EMEA) at Blue Coat Systems stated: "There have been lots of positives to come out of the Government's Cyber Security Strategy. However, let's hope there is substance behind the claims."

For Hawthorn, one such positive is that the Government is promoting 'kitemarks' for cyber security software to help businesses make more informed choices.

"It's important that we work together to encourage an 'open sharing' mentality," he explained. "There needs to be a system that anyone can sign up to, where knowledge of criminal web pages can be shared between millions of users around the world. In order to win this fight, both businesses and consumers need to share their experiences."

Hawthorn went on to say: "As the Government says that "around 6% of the UK's GDP is generated by the Internet, and this is continuing to grow", this is a stark reminder to every business owner that if they are not embracing the Internet for business, and less than 6% of their revenue is generated by the Internet, then they are behind the 'iTimes.'"

In conclusion, Hawthorn outlined: "We appreciate what the Government is trying to achieve with the Cyber Security Strategy, but what's concerning is that although leading organisational bodies such as SOCA and UK Trade and Investment (UKTI) are featured prominently, we fail to see how this is going to resonate with commercial organisations. If we're all going to work together, the Government needs to take into account many more factors, including reaching out to the private sector and enterprise organisations to fully understand their concerns and what needs to be achieved."



Sophos applauds Cyber Security Strategy effort... but warns of hard fight ahead

"The Cyber Security Strategy is a good start from the Government, and it's clear that it's not only investing in defence, but also proactive measures to disrupt threats to information security," suggested Graham Cluley, the senior technology consultant at Sophos.

"The devil is always in the detail, however, and it will be interesting to see how these programmes will be put into place, and how their success will be measured."

Cluley elaborated on that last point. "For example, when it comes to sharing information with the Government, private businesses will want to be assured that intelligence will not just flow from them to the Government, but also in the reverse direction."

From Cluley's point of view, another ambiguity is how kitemarks would actually work. "It's predictable that scammers will simply put bogus kitemarks on their sites and fake anti-virus products to appear legitimate."

Finally, with emerging technologies (such as the rapid growth of mobile and storage of data in the cloud, Cluley said: "It's essential that the strategy is flexible enough to take account of this."

He concluded: "Internet crime has become an organised, professional operation with those behind it adapting quickly to changing circumstances and exploiting opportunities. The stakes are getting higher for businesses, Governments and end users, and it's not a battle that can be won easily. Nevertheless, seeing the UK authorities treat it as a serious concern is welcome news."