Sonia Blizzard

Collaboration is the key

The idea of cyber security suggests that it is something private, not to be shared, something that should be left between the security provider and the recipient. Yet the idea of a collaborative approach to cyber security is not such a crazy one and sharing the burden of ensuring your security is running in the most up to date way might be best for your business in the long run.

Strengthening defences

Businesses and individuals who recognise the threats of hacking, online manipulation or complete loss of data are always looking for ways in which they can strengthen their defences. The route to stronger defences may very well be in preparing your security measures in collaboration with other members of your board, other departments of your business and partner corporations. The advantages of collaborating in your cyber security measures far outweigh the disadvantages, with the ability to keep on top of changes to cyber security far more likely when you are collaborating with partners or other businesses.

According to Microsoft, neither the government nor private sector businesses will be able to grasp and keep up with the changes in cyberspace when they are acting on their own and they estimate that within 5 years there will be a 50 per cent increase in the amount of data that is being generated.

These figures pose significant challenges to both government departments and private sector businesses when it comes to maintaining the security of their data storage and keeping the information which powers their business activities safe from harm.

The collaborative approach: UK

The collaborative approach does not mean that you have to give your security information to the people who work at the office down the street, nor does it mean that other businesses should be given access to your most precious data, but it does mean that a partnership should be entered into where businesses, government entities and other corporations should be looking out for each other when it comes to protecting themselves from cyber threats.

The UK government has recently launched a Cyber Security Information Sharing Partnership (CISP) which facilitates the sharing of information about cyber threats and other possible problems in cyberspace in order to make British companies more secure. This has followed on from a pilot scheme which was launched with 160 companies and proved extremely successful.

The CISP scheme includes a secure virtual "collaboration environment" where government partners and those in the cybersecurity industry can exchange information on possible threats and vulnerabilities which they have encountered. This can be done in real time, so if a threat is serious, businesses can be aware of the possibility before it breaches their cyber security measures. This partnership is supported on the government's side by the Security Service, GCHQ and the National Crime Agency, who work in collaboration to produce an enhanced and detailed image of cyber threats facing the UK for all partners.

The collaborative approach: Canada and USA

This move by the UK government is not dissimilar from a practice recently undertaken by Public Safety Canada and the Department of Homeland Security in the USA, who are collaborating to secure their joint cyber infrastructures.

The two governments, urged on by the fact that they share a border, are working together to make the cyberspace safer for citizens of both countries and those across the globe, and their Cybersecurity Action Plan will enhance the sharing of knowledge between government entities in each country, and will ensure that all partners have access to real time updates to cyber threats.

The implementation of the Action Plan will also result in the sharing of information about incident response management relating to defence and threat mitigation, and will provide other partners with help and advice consistent with

the laws and politics of each country.

The sharing of information, while primarily for the use of each government security department, will also be extended as far as the private sector industries in both countries. This collaboration will not only provide details of cyber threats and best practice in incident management, but briefings for private sector companies will be conducted jointly by each country. Private sector businesses will also have a hand in reviewing the processes for technical assistance, including the way in which information is shared and the way in which it is received by those in need of it. The Action Plan will, according to the Canadian bureau for public safety, also work on public awareness of cyber security, thereby making the safety of cyber networks a shared responsibility amongst private sector businesses, public sector corporations and individuals.

Together, Canadian and USA officials will work to ensure that citizens of both countries have up to date and trustworthy information regarding the security of their networks, and they will make sure that their awareness messages are consistent when supplying information to the public.

Cyber Security is no longer a private matter

This kind of collaboration, whether in the UK or abroad, shows us that cyber security is no longer a private matter, and that businesses as well as individuals will benefit from sharing information which helps them to remain vigilant and aware of the threats towards their companies or personal networks. Cyber security strategies are different across industry spheres, and it is clear that security should be tailored to the needs of each business.

Don't keep it to yourself…

However the latest direction in which cyber security is going is a strategy which can be implemented across all sectors - useful information which you receive is not to be kept to yourself, and likewise any information received by others should be shared equally. If the UK Cabinet Office is correct in its assessment that 98 per cent of large UK companies lack insurance to help them recover from a serious cyber attack and yet 81 per cent have admitted to an attack in the last 12 months, then collaboration seems like an essential tool in protecting our economy. As more British businesses, and those abroad, are unfortunately falling victim to groups of criminals who target these corporations for financial or identity theft, to steal their intellectual property or to seek to harm their brand, then these businesses should unite to fight against the activities of these groups. The sharing of information, no matter how small, seems to be the key to solving these problems, hopefully before they even surface.

About the Author

Sonia Blizzard is the Managing Director of Beaming – a company that provides secure internet connectivity and data back-up services to a number of businesses across the UK. Coming from a corporate background in the telecoms industry, Sonia worked for a firm which is now known as BT Global Services, setting up Beaming in 2004. The company bridges the gap between actual business needs and IT; specifically the broadband and telephone connectivity that's vital for running a business day to day.

Co-ordinates

E-mail: sonia@beaming.biz
Website: www.beaming.biz
Tel: 44 (0)1424 462661

Important Notice

Publication issued on 1 July 2015