http://www.idgconnect.com/blog-abstract/27174/better-communication-collaboration-key-beating-online-criminals-terrorists

Better communication & collaboration key to beating online criminals and terrorists

06/06/16

- Posted byDan Swinhoe
- on June 06 2017

The UK is suffering from "decision maker stasis" when it comes to protecting itself from malicious actors, according to a former GCHQ director.

"We're currently in an environment where nobody really understands what they have to protect themselves from, from whom, or why they [malicious actors] are a threat," said Brian Lord OBE, former GCHQ Deputy Director for Intelligence and Cyber Operations, at a NetEvents Security conference in London this week.

"So as a consequence, we end up with decision maker stasis at industry level where organisations don't know what to buy, don't know what to believe, and so nobody invests in anything. We as organisations have adopted the use of technology but have not invested in the security to follow it up."

Failure to communicate

So who is to blame for this stasis? According to Lord, it is a combination of the government, industry, and the media.

"Governments and industry struggle to talk to each other effectively to be able to genuinely explain what the nature of cyber risks are."

This miscommunication is partly because they view risk and threat very differently. Where governments and agencies have a very low tolerance for risk, the technology industry has a far higher tolerance. The other part, argues Lord, is down to the security industry's ability to sell itself very - and often too - well.

"There are still a lot of elements who remember 1999, when they were told aeroplanes would fall out of the sky, satellites would spin off into space, screens would go blank and the world would end as we know it."

“That didn't happen, and so as a consequence, the perception of advice and information from the IT security industry is jaundiced by history. Selling by fear never works. All we need is a responsible IT security market to sell basic tools, advise on basic control measures, and basic education, and in effect, the vast majority of that problem will go away."

Lord also called out the media for the way it portrays cyber-incidents.

“Everything from website defacement - which I call vandalism - all the way through to an attack on the critical national infrastructure - which I call an act of war - and everything that sits in between, is always reported as a 'cyber-attack'.”

“It doesn't help. It doesn't help the public understand what the problem is, it doesn't help industry understand what the problem is. No other nefarious activity has such a wide spectrum covered by two simple words.”

Criminality

“All our industry is dependent on IT, the internet, and connectivity,” says Lord. “That ability to have data now suddenly has a commoditised value to a criminal.”

He explains that around 80-85% of all hostile activity online is carried out by criminals, rather than state-sponsored or terrorist actors, but around 70-80% of that figure is done by what he calls ‘basic opportunist criminals’.

“These are low-level people with basic skills using publicly available tools just exploiting a very, very rich marketplace.”

This rich marketplace is being created by companies simply not doing the basics, and “Criminals are operating in an online sense of being able to walk into the equivalent of a town centre where everybody's doors are open, windows are open, tills are open, safes are open, cars are left there with the doors open and the keys in and no one is watching.”

“If one looks at the NHS two weeks ago, the impact of that could have so easily been avoided by basic proactive measures: basic maintenance; patching. If businesses and governmental organisations do basic things correctly will raise their health - their hygiene - above the threshold of most opportunist criminals.”

If we strip away the opportunists by doing these basic things correctly then agencies, organisations, and vendors can focus on what Lord calls the serious and organised crime groups.

“They are not interested in opportunistic crimes, they are looking at getting to the heart of the banking systems, the payment systems. The general view from most serious organised crime groups at the moment is any single operation needs to be able to yield £1 billion for it to be worthwhile.”

State-sponsored attacks

While weaponising new technologies are not new – and something most countries are interested in - state-sponsored attacks aren't nearly as common or sophisticated as is often suggested.

"The view that at the moment states have the ability to, at random, take down critical national infrastructure in a meaningful way is not the [current] position."

He says that states are working towards that goal, and will eventually get there, but currently it isn't as dramatic as is often perceived.

"Being able to develop coherent, coordinated attacks against critical national infrastructure in a way that delivers a very specific sustainable effect is extremely difficult to do, it's extremely expensive to do, and it involves a huge amount of effort."

Terrorism, and social media companies vs responsibility

In the wake of recent attacks in London and Manchester, the subject of terrorism is hard to avoid. But rather than talk about Theresa May and her issues with encryption, Lord is more focused on social media companies and their role in enabling terrorists.

"When we talk about cyber-terrorism we should not get distracted by thoughts of trains coming off tracks or aeroplanes falling out of the sky," says Lord. "To be able to attack and take down critical national infrastructure is not in the capability or mindset of terrorist organisations."

Instead, says Lord, terrorist organisations use the internet as means to gather money for their cause via criminal activities and to fuel their propaganda via social media and online radicalisation. And because of that, social media organisations need to work harder to prevent this and work more closely with governments.

"It is not a sustainable position for social media organisations to not do anything about online radicalisation, nor is it sustainable for them to continue to withhold any degree of cooperation for law enforcement."

While he says that agencies simply getting everything they want as soon as they want it won't happen, there will be a change in the relationship between them and the social media organisations.

"They are still very young organisations. They may be global, they may be huge, I do not yet think they understand their responsibilities or the influence they can and can't have. But they cannot anymore operate in this singular view which is 'hey we just provide a platform'. That is not a supportable position."