The rise in cyber attacks shows we need to change the way we think about crime

July 26 2016, by Daniel Prince

Credit: AI-generated image (disclaimer)

You are now 20 times more likely to have your money stolen online by a criminal overseas than by a pickpocket or mugger in the street, according to recent figures from the Office for National Statistics. The figures, revealed that almost 6m fraud and cyber crimes were committed in the past year in England and Wales alone – making it now the most common type of crime experienced by adults in the UK.

It is the first time fraud questions have been added to the official Crime Survey for England and Wales – and while it has been known for a long time these figures would be significant, it is clear many people didn't realise just quite how significant they would actually be.

In fact, the release of the figures led to police chiefs calling for a national campaign against online fraud and other cyber crime on the scale of last century's seat-belt and drink driving campaigns.

At the moment, if you are a victim of a cyber crime, contacting Action Fraud – the UK's national fraud and cyber crime reporting centre – is the main way of logging it. The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau who are responsible for assessment of the reports and to ensure that your fraud reports reach the right place. And yet, despite all this, within law enforcement and the cyber security industry we know cyber crime is still significantly under reported.

Tackling cybercrime

Back in 2013 I worked on research looking at how people report and measure cyber crime. It identified that the government, local authorities and police and crime commissioners would not allocate resources to tackle the problem until the true scale of cyber crime was known. Now three years on we have the evidence, we know the scale of the problem – and now we need to respond.

There is, however, a significant challenge in responding to cyber crime, which is a lack of specialist cyber skills – such as forensics, investigation, prevention and victim care. And due to this shortage, cyber security experts often command a premium salary. But while schemes such as "cyber-specials" engage these skills in the private sector to support the police service, it is not just the specialists we need to think about.

The average frontline police officer also needs to be able to think about the digital crime scene as well as, or instead of, the physical one. Being able to respond and investigate criminal cyber activity should no longer be the domain of police specialists – because, as the evidence shows, victims are more likely to suffer a cyber criminal act than any other form of crime.

Police and crime commissioners need to factor this into their plans, and specifically work with their law enforcement organisations to understand the local picture. This local understanding is important as there is less clarity on cyber criminality at a regional level – and it is this clarity that will drive local policy and resourcing decisions.

Stronger together

Beyond law enforcement, society must think about the role of the private sector and their duty of care. Everyone online is sitting on an internet service provider's network, which effectively owns the digital land upon which we have set up our digital lives. In the physical world, landlords renting a property have a duty of care to the safety of their tenants, so surely it makes sense for our digital landlords to be held to the same standards.

Perhaps this is a market issue, and market forces will drive customers to think twice and consider things like cyber security when choosing their provider, rather than just costs and internet speed. However, this won't happen until the companies in charge of this digital landscape provide more transparency on the level of attacks their customers experience – which current legislation does not require. But this situation cannot continue, and examples such as the Talk Talk hack demonstrate customers can and will move to companies that can protect them.

To respond effectively we need to look at the data gathered on the nature of these crimes – to understand how cyber crimes occur, and who is most at risk. In the long run, this will make it easier for law enforcement to work out how to tackle these cases.

But this must be done in a sensible and measured way, as the situation is likely to appear to get worse before it gets better as people become more aware of what these crimes are and how to report them. Similarly organisations, such as the ONS and the City of London Police, will get better at recording cyber crime – causing the figures to go up again. For now though, these new figures make it clear that cyber crime must become a significant priority for the police and crime commissioners up and down the country.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: The rise in cyber attacks shows we need to change the way we think about crime (2016, July 26) retrieved 11 July 2024 from https://phys.org/news/2016-07-cyber-crime.html