HUFFPOST TECH
UNITED KINGDOM

Happy New Year! The Only Thing We Have To Fear Is The Lack Of Fear Itself

12/01/2017 16:37

Dmitry Bagrov Managing Director UK of global technology consultancy DataArt

OCUSFOCUS VIA GETTY IMAGES

Every post you make, every breath you take, every search you make, *they'll* be watching you. Every bit of information you have ever entered anywhere online is stored, collated and held. For the most part, we give this data over without even thinking about the consequences, assuming it is safe.

If you think you are protected, if you think you have taken every step to keep your data safe, if you think, just because you take all precautions possible, you cannot be attacked, you are wrong. In truth, unless you have somehow managed to have no data online (which if you are reading this would be next to impossible), you *are* at risk, you *are* exposed. As the former FBI Director Robert Mueller said in 2012 "There are only two types of companies: those who have been hacked, and those that will be."

The internet has often been likened to the old American Wild West, with very few rules governing what goes on. However, in recent years this has begun to change. As technology has progressed, governments and corporations are slowly giving structure to the internet. A reappraisal of the modern online landscape shows it is clearly no longer bandit country but one governed by major forces be they nation states or powerful corporations. Much like the world itself. And like the world, it has a dark underbelly of thieves and criminals. However, unlike in the real world, where we have a system of law and order and locks to keep us safe, online we are completely exposed.

In 2010 a website called pleaserobme.com launched to brutally demonstrate the security flaws in social media. This website used publically available information on people's locations, taken from Facebook, Twitter and other social media with geotagging to highlight when people were not at home. For example, if you lived in London but had recently announced your arrival at JFK Airport with all the family, chances are your house was empty and much easy to rob. The controversial site showed this with shocking results.

Now seven years on, the issue has not improved. Data is still easily available and not only could it expose your house to being robbed but your entire life could be stolen. There are countless examples of people losing nearly everything from online fraud, or from having their data accessed.

This level of risk exposure goes way beyond tech issues, though those do exist: it strikes at the very heart of how we live now so much of our lives are online.

Imagine waking up one day to realise your front door cannot be locked, there is a hole in your wall, the roof of your house is missing and it's all your fault. Feel safe? I think not. The blunt truth is our online lives are as exposed as our physical one and we are living in houses with no doors. For the past few years we have been living through an age of wishful thinking, believing that we are safe or that cyber security problems are small and will be solved, and it will all work out in the end.

This wishful thinking comes down to an organisational mindset across governments and companies the world over, that treats technology as just another commodity. People are assuming that tech can be treated like everything else, what we 'do'. The reality is that it is at the core of entire lives. It is what we are.

Until we achieve a shift in mindset that recognises this fact, and leads the world to act accordingly, the issue of cyber security exposure will never really be solved. As we make our way into 2017 we have not even started to approach the concept of being safe online. Our companies, our lives and our governments are exposed to terrifying risk, and ultimately it is all our own fault. By failing to adapt our awareness, change our assumptions and shift our thinking to the new world order we have left ourselves open to attack.

Only with such a shift can the problem of cyber security really be tackled. It is not a matter of resources, as Richard Bejtlich, Chief Security Strategist at cybersec company FireEye, once outlined; for $1 million a team could be assembled to hack any target. But $1 million wouldn't be nearly enough for a company to protect against attack.

To reiterate, technology is such an integral part of our lives that the assumption it can be treated as an added extra, or something to bolt on, rather than at the very core has left us completely open to a catastrophe. This may never happen, but the clear and present danger will always be with us until our collective mindset changes.

Even if we are never the victims, the threat is always there. Even if we take all possible precautions, others will leave us open to attack. To quote the late, great Joseph Heller: "Just because you're paranoid doesn't mean they aren't after you." In 2017, I hope we realise they are after us and take the actions needed to become safe.

Follow Dmitry Bagrov on Twitter: www.twitter.com/dmitrybagrov

Original article — http://www.huffingtonpost.co.uk/dmitry-bagrov/happy-new-year-the-only-t_b_14081036.html