# WILL THE ROBOTS WIN?

**Paula Mathers** *considers the impact of the growing trend for using AI as our workforce*

**Paula Mathers** worked for six years as a cross-cultural psychologist for the British Government. She joined CoverGuard Security in February 2016 as the company manager and was promoted to assistant director in September 2016.

**As a society, we seem to want things at the touch of a button, from our smartphones and without having to see an actual person. We can arrange loans, overdrafts and mortgages using our mobile phones and tablets, we can buy a house without even leaving our living room and how many of us have done our weekly grocery shop while sat in the bath? The use of apps such as Facebook, Twitter and online banking have left us expecting others to give us the answers we want without waiting, and without having to deal with queues and appointments. We can do whatever we want from the comfort of our own homes with a cup of tea in our hand.**

Looking through banking news online, I discovered that Bridgewater Associates – the world's largest hedge fund – is set to replace its managers with artificial intelligence to complete tasks from strategic decision making to the hiring and firing of staff. Dutch banking is set to replace 5,800 people with machines, at a saving of $1 billion a year. Germany's Commerzbank has announced that by 2020 it will digitalise and automate 80 percent of processes. Although I'm not crazy enough for that to give me visions of a cyber version of *Planet Of The Apes*; the world being over run by robots, it does make me worry about the security of these plans and what it means for the regular customer.

On 19 April 2017 *The Telegraph* (online edition – of course, so I don't have to leave my house and see any actual people) reported that as many as 46 percent of UK businesses were hit by a cyber attack or breech of their computer systems in 2016. The cost of these attacks ranged from £1,570 through to £19,600 for larger businesses. One business in particular reported it had received 340,000 fraudulent emails in that year alone. Some of these cyber attacks have been quite high profile; for example Three Mobile and Tesco both reported losses of customer data as a result. This data would have included bank details, home addresses, dates of birth; enough information to steal a person's identity if the attacker so desired. Swapping physical people from our staffing registers to artificial intelligence and computers isn't going to make this any better. We don't have enough cyber security in place, or effective enough security to manage what computers we do have, let alone replacing 10 percent of our entire workforce (*The Telegraph*, 2016) with computer technology by 2020.

Here in the UK, we seem to have a false sense of security; we seem to believe that significant data breeches only happen in the United States, as that is what is reported to us in the media. This is because US law forces organisations to report such data breeches; something that is not the case in the United Kingdom. Here, organisations worry more about breeches to the Data Protection Act, as that is what will cause them to lose their accreditation. In actual fact, the UK ranks second in the world for data breeches, with many of the most significant ones having happened in the last two years. The most recent data breech to have a significant impact within the UK, is the computer virus that infected NHS computer systems in May 2017. Not only did this ransomware infect 47 NHS England Trusts, but it also affected hundreds of companies across the world. NHS staff found themselves having to go back to the old paper and pen method of updating patient records, cancelling appointments and (non-urgent) operations, throwing the entire country into panic.


**Yahoo is the latest company to have suffered from wide-scale hacking**

The popular payday loan company, Wonga, also fell victim to hackers in 2017. It suffered from a data breech that saw the details of 245,000 customers' details released, including back account numbers, sort codes, email details and home addresses.

And that's just a couple from this year. How many physical staff members in your company have stolen information? How many 'customers' have written fraudulent letters? I'm guessing the number is less than what we see on the cyber side of things. The last time we saw an industrial revolution was in 1760 where the only risk was machines becoming jammed, or a lack of oil on the equipment. That was a risk that was mitigated back then and we learned from it. We aren't developing anti-ransomware and anti-virus software fast or robust enough to follow through with this modern day industrial revolution. If we continue to replace human staff members with computer systems, our cyber security is really going to have to step up its game ●

Picture credit: Getty