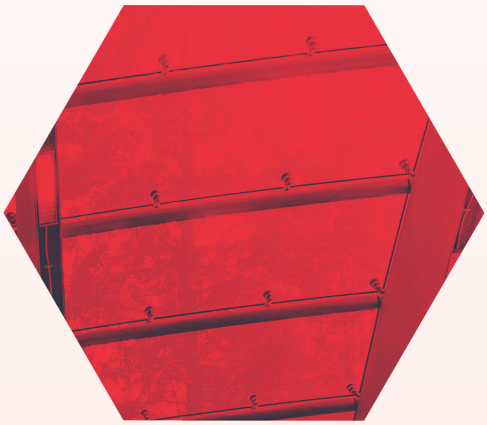
Looking Forward to 2019

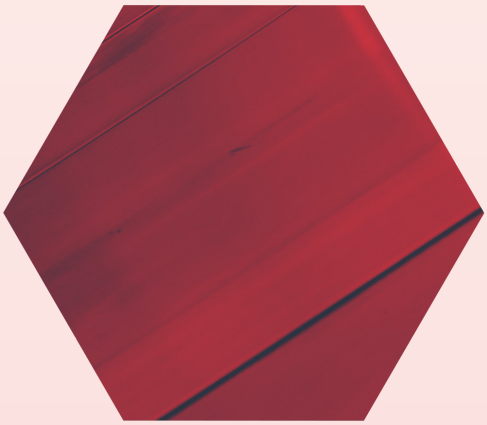
Over the past few years we have witnessed the cyber security industry evolve dramatically. We've seen sophisticated breaches on large companies causing detrimental damage as well as high profile attacks on the government. With cyber security being a taboo topic the past couple years, the general public's knowledge of the industry has shifted to a more in-depth understanding of the perils of poor data practice.

Making predictions for the coming year is especially tough in an industry like cyber security. The threat landscape is huge, offensive, and the sophistication of attackers is improving rapidly.

As a result, the information security industry experiences extreme pressure to keep up with the ever increasing cyber risks. This leads to the industry evolving and changing and an unusually fast pace.

These rapid changes in the industry make it hard to see or asses every trend. Still, there are some industry issues and trends we able to foresee into the next year. These include the skills shortage, the gender gap and the effects of Brexit.





Skills Shortage

Despite the well cited skills gap within cyber security, do not believe the tales of 0% unemployment. At any given time, our consultants can speak to a number of competent and experienced security professions who find themselves out of work. As an industry, our problem is indicative of, but not made of a skills shortage. Rather the problem is a hiring shortage.

Throughout the next year, we will likely witness companies struggle to fill their security teams, competing for the same top talent. As a result, the salaries will likely increase yet again, and will continue this way until companies begin training and promoting in house.

With the market particularly competitive for permanent employees, factors such as speed-to-offer and engaging candidates with the security roadmap, can become decisive. A well-defined role with a vision for the medium term is an essential part of attracting and retaining security professions. Given the importance of the industry and the responsibility attached that comes with the job, it is only right that we understand the situation, strategy and commitment of the employer.

Gender Gap

The industry is slowly moving in the right direction, with the percentage of women in the cyber security work force up from 11% in 2013 to 20% some 5 years later. However, it is clear there is still a long way to go. Throughout the past year, the tales of sexual indiscretions and inappropriate behaviours reverberated around major industry events are abhorrent. This is not only limited to the cyber security industry, but across nearly all industries. After the #MeToo movement, it has become clear that societal perceptions of women in the work place are still unacceptably sexist which is inexcusable.

As an industry, we need to be vigilant in deterring any form of this sort of behaviour. If we cannot overcome this imbalance, we risk not only driving away those already in the industry, but also

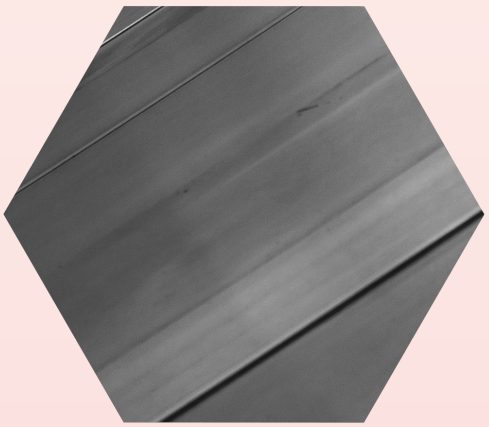
deterring the next generation of cyber security professionals. With aforementioned mentioned skills shortage, we have yet even more motivation by which to combat it. By improving the percentage of female information security professionals, this gap will hopefully be nudged closer.

Fortunately, broadly speaking in security we are fortunate to have acknowledged there is a problem. As a result there have been numerous membership organisations and groups discussing and campaigning for equality and to increase the numbers of women entering the profession. In the coming years we can hope that with these contributions and recognitions, attitudes will change and the percentage of women in the workforce will improve.

Brexit

While we still wait to see what the UK's divorce settlement from the EU might entail, it is hard to make predictions for the coming years on the impact this might have on the industry.

An issue we are likely to face is the movement of data between the EU and the UK. In the event of a 'no deal' brexit being reached, the EU will effectively be refusing to begin the process or preliminary discussions until the point that the UK becomes a third nation. This would mean that companies will have to mirror GDPR in to standard contractual clauses and may be required to appoint representatives overseas in the EU.



In the long term, it will be imperative that the UK remains an attractive destination for European professionals, trade agreements will remain commercially attractive enough to continue to draw organisations to base themselves here. Deal or not, new agreements and legislation will come eventually, so any worse case scenario is likely to be temporary. The UK will continue to host international companies, and we will (for now) continue to be Europe's biggest data market. In a logical world, security teams should typically be based where the data is and you would expect companies to continue to use the infrastructure and personnel they have invested in where possible.