How safe are our elections?

In recent years, several allegations have been made suggesting overseas interference in the Brexit referendum and UK general elections, not to mention ballot fraud, all with the aim of manipulating election results. Alleged election tampering reared its ugly head again over the local elections held on 5 May 2022, both in terms of cybercriminals attempting to tamper with results by hitting processing systems as well as conducting online harassment targeting political candidates to 'skew' public votes.

It is particularly difficult to assess the impact of such reputational damage, how tampering or harassment took place and linking those activities to cybercriminals who inevitably shield behind online anonymity. This often involves having to trawl through numerous offending posts, activities, and accounts in an attempt to draw any connections or patterns and then, where appropriate, pursue other more advanced means and/or work closely with law enforcement to bring those parties to account.

The plethora of attempts online and through social media to sway public opinion is nothing new, though strikingly, there are more bold and brazen attempts to make pre-empted, rehearsed, and often targeted abuse online towards individuals and public authorities. These attacks are politically motivated with purpose and sometimes have dire consequences, including even loss of life. This is a very scary trend, coupled with the seemingly rising number of state-backed cybercriminals attempting to hack public authorities through encryption and exfiltration or Distributed Denial-of-Service (DDoS) attacks.

As this type of activity increases, it is more imperative than ever to have appropriate experts on-hand to deal with any incidents that occur, as these attacks can be very costly and can cause irreparable reputational damage.

Our Cyber team works closely with our in-house Special Investigation Unit and external cybersecurity partners, to investigate these claims and, where possible, bring those offenders to account. We utilise our 24/7 Cyber Incident Response capabilities, together with our specialist cyber adjusting and claims management services to provide our clients with a streamlined and cost-effective solution. Our partnership with CyberClan has enabled us to extend our capacity, going the extra-mile for our clients and providing flexible options for all budgets.

This dangerous trend is not going to abate any time soon and fighting this together is the only option!

Author: Will Gow, Head of Cyber and Financial Lines.