ASSESSING THE CYBER RISK LANDSCAPE FOR PRIVATE CLIENTS

High Net Worth (HNW) and high-profile individuals, including actors, sports stars and celebrities, operating in an increasingly interconnected, scrutinised and 24-hour covered world are progressively under threat from cyber security risks.

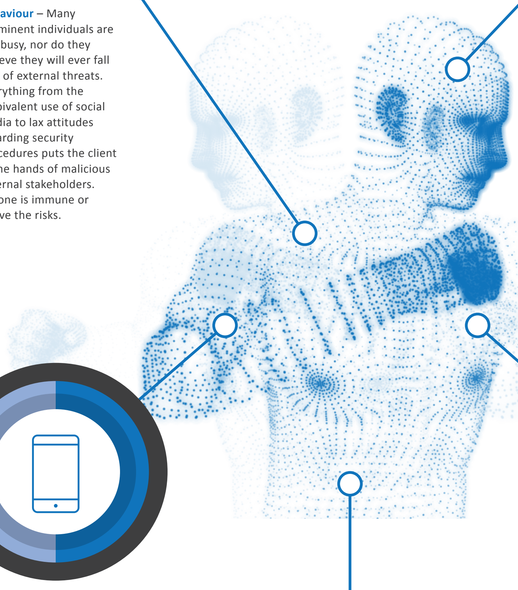
As highly valued targets in a treacherous digital landscape, private individuals require support and expertise in safeguarding not only their reputation and brand but also their physical security, privacy and commercial assets.

Cyber criminals, hacktivists and digital influencers operating on the open, dark and deep web are increasingly targeting prominent individuals for either financial gain, exposure or simply for notoriety.

Cyber security protection is, however, greater than just technology. Rather, strong cyber defences can only be built with solid governance, education and procedures not just for the client but their wider team, stakeholders and family.

With comprehensive expertise and support, private clients can gain confidence in the knowledge they are best placed to protect their brand, privacy, security and finances in the face of increasing global cyber threats.

5 key threat vectors putting your clients at risk:



Behaviour – Many prominent individuals are too busy, nor do they believe they will ever fall foul of external threats. Everything from the ambivalent use of social media to lax attitudes regarding security procedures puts the client in the hands of malicious external stakeholders. No one is immune or above the risks.

Email – Email remains the main cyber-attack delivery mechanism. Common techniques include social engineering and phishing. As highlighted by the spate of recent ransomware attacks, malicious emails are an easy and highly effective way to breach the client's defences. Once compromised, attackers can operate within a target's network, extract personal data/information and extort money at the expense of a client's reputation and wellbeing.

Mobiles Devices – Today's mobile phones are more powerful than most laptops. They provide access to a vast range of data and personal information. Despite this, many individuals rarely think about updating anti-virus software on their device, using comprehensive passwords, or the use encryption on their devices. Mobile devices remain a soft target for many hackers wishing to do harm.

People – Stakeholders, staff or family members remain a vulnerable and not immediately obvious route in which hackers can target and compromise prominent individuals. Devoid of sound governance and procedures, a client's reputation, privacy, assets and security remain at risk.

Governance – Cyber "negligence" from leadership is no longer excusable. HNW individuals typically lead a wider network of stakeholders directly or indirectly affiliated to their daily life, brand or business. Good cyber governance is required to permeate from the top, extending to and beyond everyone within a client's inner and extended circle. All parties need to be educated and made aware of the external risks and dangers.