Digital Risk Protection for High Net Worth Individuals

There is less separation than ever before between our digital and physical worlds.

While this exposes everyone to scams, identify theft and other forms of cyber crime, high net worth individuals are exceptionally vulnerable to these risks – and the risks are increasing in seriousness and frequency all the time.

The digital line between a high net worth individual's personal activities online and their professional life is also blurring. For example, threat actors have already damaged many organisations by creating a convincing digital impersonation of their CEOs, often by using information taken from personal social media posts.

Disturbing "kidnapping" scams, for example, have been made possible by the rapid advances in artificial intelligence, which can draw on the huge amount of publicly information available about high profile people and their families.

Impersonation fraud cost an estimated

US$5.3 billion

in 2022

Source: FBI

Incident Response Hotline: +44 (0) 207 459 4888

Tel: +44 (0) 20 8057 7100 | Email: cyber-enquiries@thomasmurray.com | cyber.thomasmurray.com

Global Cyber Risk Services

Thomas Murray

Thomas Murray Digital Risk Protection (DRP) is the first service to address the unique dangers faced by high net worth individuals in this ever-changing online environment.

It is dedicated to protecting high net worth individuals, senior executives and other high profile stakeholders, along with their families.

DRP is designed to assist in protecting assets and information that are outside the physical and logistical control boundaries of corporate environments – including personal devices like laptops, mobile phones, smart home devices, personal email accounts, social media accounts and so on.

- **A scalable, bespoke service** with the option to include friends and family
- **Personal IT audit** – an audit of all physical devices owned or used by the individual (and their family), personal network discovery, email account configuration, online banking setup etc.
- **Identity monitoring** – monitoring of leaked/breached personal credentials, and of social media accounts for impersonations and doxing
- **Device monitoring** – monitoring of personal devices for malicious activity, software, or applications
- **Device management** – manual/automated secure configuration management of personal devices, along with smart home devices
- **Credential monitoring** – credentials searched for in dark web datasets
- **Response service** – 24/7 response to instances of untoward incidents
- **Cyber concierge services** – Dedicated cyber and IT support

To find out more contact:

Cian McDonagh

Business Development Lead | Cyber Risk

+44 (0)20 8057 7248

cmcdonagh@thomasmurray.com