blenheim partners
no limitations
Executive Search & Board Advisory

THE THREAT OF CYBERTERRORISM – ORGANISATIONS ARE VULNERABLE

Cyberterrorism is the use of the Internet to conduct acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation. It is also considered cyberterrorism when activities including deliberate large-scale disruption of computer networks, such as personal computers attached to the Internet are attacked by computer viruses, computer worms, phishing, and other malicious software as well as hardware methods and programming scripts as a means to create significant turmoil to the State, community and business.

Experienced cyberterrorists are very skilled in hacking and can cause tremendous damage to government systems including hospital records, national security programs, and public infrastructure which might leave a country, community or organisation in disarray. They can even potentially change the course of a nation. The 2016 US Presidential elections saw an attack from Russian hackers targeting voting systems in numerous American states with the National Security Agency unable to stop it. Other countries with less sophisticated safety measures are increasingly becoming a vulnerable target and have already felt the effects of cyberterrorism in different forms and paying a hefty price.

In May 2017, the WannaCry ransomware strike spanned more than 150 countries and targeted public utilities, large corporations and 230,000 computers. It crippled the National

Health Service hospitals and facilities in Britain. Russia, Ukraine, India and Chinese Taipei were the worst affected countries costing billions in damage. The WannaCry attack showed to the world the rapid; global damage cybercrime could cause. A month later, Petya ransomware struck multiple countries including Australia, with courier companies, legal firms and even Cadbury and its parent company Mondelez being afflicted. Researchers suspect the Petya ransomware masked a targeted cyber-attack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities including power companies, airports, public transport and the central bank.

Australia's critical infrastructure is coming under attack by foreign hackers several times a day. The criminals have enhanced their methods, using ransomware where they lock down computer files, employing encryption then demanding payment in hard-to-trace cryptocurrencies. Other methods include weaponisation of AI with machine-learning being used to rapidly strike unsuspecting organisations with greater reach and without human constraints.

The cyberterrorists are not limiting their efforts to national targets but are also focusing on business with an increased and alarming intensity. Over the past few years, the world's stock exchanges have observed and experienced an increasing threat of cyber-based attacks, with hackers being bolstered by the increased refinement and availability of destructive tools. In 2017, Equifax, a global corporation had an attack that led to the leaking of private customer information including Social Security numbers and other critical data.

With most equity markets in the world experiencing all-time highs, capitalist economies are under great surveillance and threat by the cyberterrorists. Targets of terrorism could further evolve with the trillions of dollars in asset values potentially inspiring hackers to launch major scale cyber assaults stealing private information and placing organisations and investors at risk. While some proclaim large financial institutions and leading corporates are relatively immune given the vast sums invested in cyber defence, the criminals in question are becoming even more sophisticated, well-funded, and should not be underestimated.

As cyber-attacks are doubling more recently, super cyber-attacks are anticipated to become more prevalent in 2018. Cyber terrorists are expanding their target range to include industries which have become more reliant on smart technology such as airlines, vehicles and more broadly manufacturing. As a result of cyberterrorism, Boards and CEO's are genuinely concerned with the multitude of risk that cyber-attacks bring and whether their organisations are exposed and placed in harm's way.

The demand for superior technical expertise and overhaul of organisation security/risk safeguards has escalated. The price for leading top technology executives with cyber credentials has risen and the supply has fallen. Many organisations are coming to the realisation they may need to source from offshore and not necessarily in the traditional hunting grounds. This also brings with it issues in regards to security clearance.

At Blenheim Partners we recognise the impact of appointing the wrong person to an organisation will be significant and cannot be underestimated For most the challenge has not only been the limited supply but the over exaggeration of many potential candidates in

regards to their track record in this area. Blenheim Partners has invested in leading research capability and is partnering with organisations in the identification and acquisition of leading cyber/technology experts in a new and opaque market.

We would be pleased to provide you with a more in-depth briefing on cyberterrorism and other technology/data/digital insights at your convenience. Please contact Joseph Marsella at joseph.marsella@blenheimpartners.com to arrange.

Blenheim Partners specialise in:

- Executive Search;
- Non-Executive Director Search;
- Board Strategy and Structure Consulting;
- External Succession Planning; and
- Executive Re-Engagement / Transition.

Founded in 2012, our team have acted as specialist adviser to many of the world's leading corporations on Board and Executive performance, capability and succession planning.

Our consultants have worked with clients from all sectors and a broad range of geographies. They include over 80 of the ASX 100, 10% of the FTSE 100, Private Equity, Multinational, Private Family and Mutually Owned Companies.

Our work includes assignments that are both local and international in scope.

Our team consists of senior Search Consultants, Human Resource Directors, Psychologists, Coaches and exceptionally experienced Researchers.

Blenheim Partners is continually investing in knowledge and understanding as exemplified by our Thought Leadership "The Challenges of Attaining Growth", Industry Papers and monthly Market Intelligence reports.

Our philosophy is to develop deep and committed relationships with a select number of clients and help them deliver a superior performance by optimising the composition of their Board and Executive team.

Our culture is built on pride, professionalism, esprit de corps and client service.

blenheim partners

no limitations

Executive Search & Board Advisory

Contact us
Sydney p +61 2 9253 0950
Melbourne p +61 3 9653 9510
w www.blenheimpartners.com