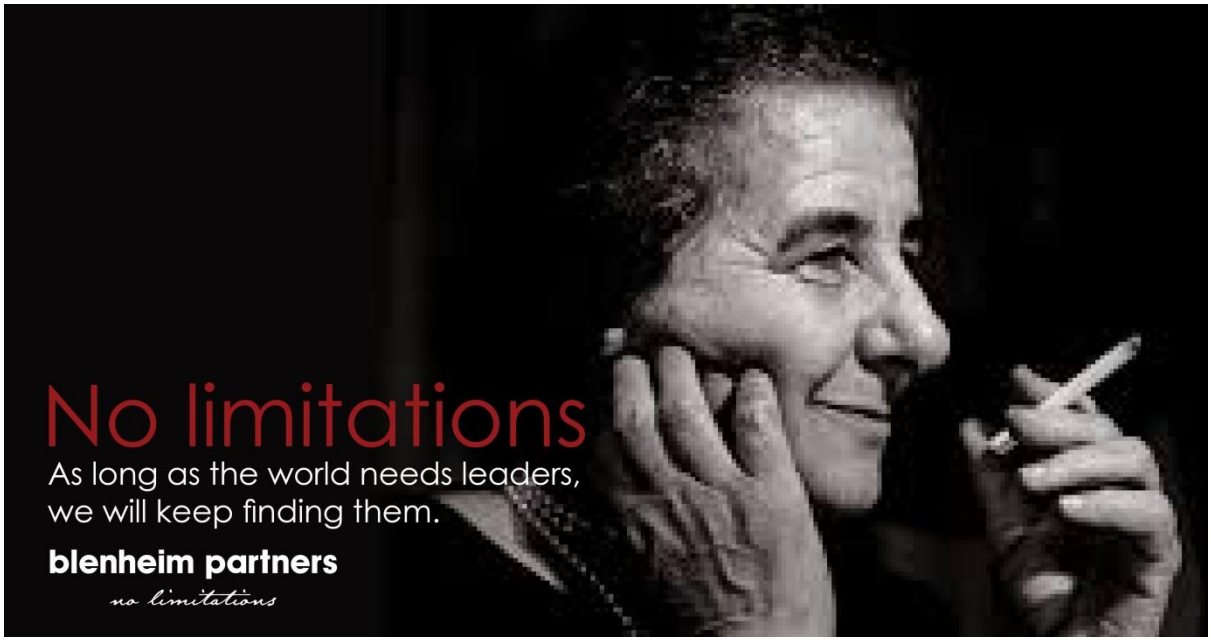
blenheim partners
no limitations

Executive Search & Board Advisory

IT PAYS TO BE IN CYBERCRIME



Cybercrime is now the no.1 economic crime in Australia.

With the dramatic increase in technology hacking, particularly in regards to money laundering, technology and security breaches, stealing of intellectual property and disruptive viruses, the demand for professionals to combat this has risen significantly.

We also have an increased concern of terrorism and general crime activity that is forcing companies to adopt new methodologies to prevent such events.

The risk for all organisations and individuals who rely on technology, is that they are all a potential target. The level of sophistication has increased and the techniques used to break though security checks are advanced, forcing organisations across all sectors to review their security walls.

Those that have expertise in cybercrime have witnessed the shift in the demand and supply curves. As a result of the increased demand and limited supply of cybercrime professionals, it is anticipated that remuneration levels will continue to rise. With recent well known organisations locally and internationally having security breaches, and banks fearful of money laundering and fraud, the cybercrime professional is now in high demand.

Like all professional roles, the remuneration will be a reflection of the scale of the remit, that is, the industry, organisation, and team size as well as level of focus on the role.

However, cybercrime specialists are very much in vogue. The demand for data specialists, those that understand the dark side of the web, those that can detect patterns, and those that can prevent large scale criminal activity via technology are being hotly pursued.

The statistics of what companies know and what they have estimated that they do not know of cybercrime incidents is disturbing to say the least.

As a leading Board Advisory and Search firm, we have been tasked to act for clients in identifying expertise in this sector. The challenge is, Australia has a limited pool of people and international experts need to be taken into consideration.

The most recent statistics include:

- Over 60% of all Australian local companies detected security incidents within their organisations; and,
- The cybercrime rate of incidents has doubled in the last 12 months.

Ransomware which is a type of malware that prevents or limits users from accessing their system, either by locking the systems screen or by using the user's files unless a ransom is paid – is more prevalent than ever. It is a lucrative business and one of the most common attacks against business and individuals. More concerning is that what used to be the domain of smart criminals is now in the hands of just criminals who can purchase ransomware off the internet.

Over fifty percent of organisations experienced a ransomware attack, over thirty percent had a business email attack in the last year and the Distributed Denial of Service (DDOS) network attacks has increased by more than two hundred percent.

Australia's high usage of technology and its economic standing make it a leading world target for cyber criminals.

Approximately sixty percent of Australian businesses have experienced ransomware in the last twelve months and over a quarter are experiencing one monthly. Those organisations based in Australia have been more likely to pay the ransom than those in parts of Asia, and less than one third of the Australian organisations that did pay the ransom did not recover their files.

Online fraud and scams make up approximately fifty percent of cybercrime reports. As a result, the Government launched the ACORN in November 2014 as a way for the public to report cybercrime. It is also used as a national intelligence database for authorities to identify and prosecute criminals.

As the digital world grows and Australia's reliance on technology increases, online transactions, engagement and information exchange is going to have to direct correlation in the incidence of cybercrime.

It would appear from the numerous sources that Australia and many Australian businesses are not prepared for cyber-attacks. The epic failure of the Census on August 9, December 2016 highlighted the failure of the nation's first e-Census.

Cyber infringements are real and present, and range from state sponsored criminal activities by nations attempting to gain intellectual property or political advantage, to organised crime syndicates and individuals looking to profit from stealing people's information, to ideologically driven activism.

In 2014, Yahoo admitted to experiencing one of the largest data breaches, when it was hacked by a state sponsored actor who stole more than half a billion usernames and passwords of its customers.

In 2016, we saw one of the more damaging cases of DDOS, which is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. This happened against U.S. company Dyn, which controls most of America's internet infrastructure. It led to outages of major websites including Twitter, Airbnb, Amazon, Reddit, and the New York Times to name only a few.

We've seen a data breach of major Indian Banks – an estimated 3.2 million debit cards compromised, resulting in the country's banks announcing the blocking and replacement of almost 600,000 debit cards.

Ninety percent of Australians will be online by this year, and by 2019, it is anticipated that the average Australian household will have over twenty devices.

In April 2016, The Prime Minister Malcolm Turnbull announced Australia's cyber security strategy. The Federal Government will invest over $230 million over four years with Alastair MacGibbon, formerly part of the Australian Federal Police being appointed as a special adviser. Mr MacGibbon's concern is that the impacts of cyber security threats are not well understood.

Cybercrime is now the no.1 economic crime in Australia. Between July 2015 and June 2016, CERT Australia which sits within the Attorney-General's department and is the main point of contact for cyber security issues affecting Australian businesses, responded to 14,804 cyber security incidents. 418 of these involved systems of national interest and critical infrastructure. The Australian Payments Clearing Association figures found that fraudulent payments cost the Australian banking industry $469m in 2015, revealing a thirteen percent increase.

Gregory Robinson, Managing Partner, "In a recent study in regards to cybercrime, it has been found that compared with France, Germany, Israel, Japan and Britain, the cyber skills shortage is most harshly felt in Australia, with suggestions that close to ten thousand cyber

specialists are required today. Executive involvement in cyber security and criminality has increased and as a result, organisations have invested more heavily in their technology and security spending. With the rapid increase in cybercrime, the result is that those in a technology security profession are in one of the most under supplied professions. As such, the remuneration increases have reflected the increased demand. It pays to be in cybercrime."

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