MAGELLAN
EXPERTS IN GLOBAL INVESTING

June 2017

Cybercrime is a growing menace

The worth of the internet is at stake

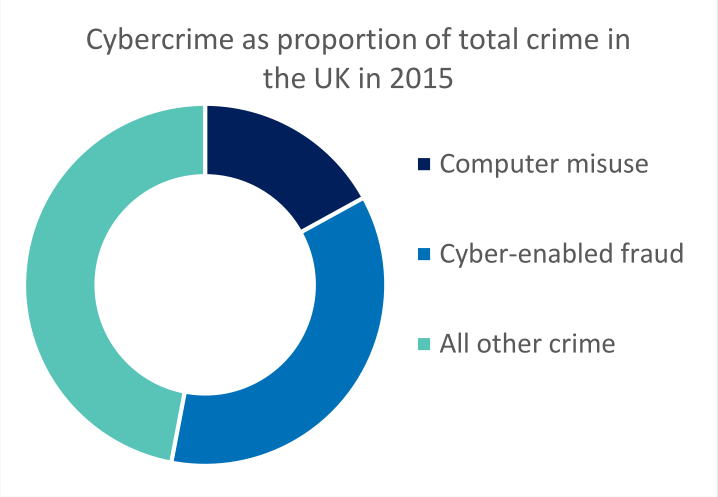
In mid-April, the 'Shadow Hackers' online group made public some malicious software known as 'EternalBlue' that had been stolen from the US government's National Security Agency, which develops hacking tools to gather intelligence.[1]

About a month later, 'ransomware' incorporating the bugs penetrated perhaps 300,000 computers running outdated Microsoft software in an estimated 150 countries. On entering a computer system, the cryptoware exploited a Windows flaw and sped through local networks via file-sharing structures.[2] On infected computers, data became encrypted and owners were told they needed to pay a ransom in the untraceable online Bitcoin currency to have their files unscrambled. No payment and the files would be deleted.

Luckily the ransomware, dubbed WannaCry, was quickly defused. But the speed and extent by which the malware spread, WannaCry's household-name business victims such as Nissan and Renault, its disruption of the UK's medical services and its ability to destroy data made the ransomware the most chilling cyberattack ever. But it's perhaps not the most significant cyberattack ever. Many claim that emails hacked from Hillary Clinton's presidential campaign and released via Wikileaks helped Donald Trump become US president. Republican Senator John McCain has called the incident "an act of war" by Russia's government, which is accused of financing the cyberattacks.[3] In the last week of the French presidential election in May, hacked material from the campaign team of the eventual winner Emmanuel Macron was published in an apparent attempt to sway voters.

Other notorious incidents of cybercrime include this year's malware attack on the US Chipotle restaurant chain that stole credit-card details from an unknown number of customers. In 2016, MySpace suffered the theft of about 350 million passwords and emails while hackers robbed US$81 million from the central Bangladesh Bank by hacking into the international money transfer system.[4] In 2014, hackers snatched about 500 million account details from Yahoo, stole details of about 47,000 employees and actors from Sony Pictures Entertainment, pilfered more than 100 million customer details from eBay and stole credit-card information from 50 million customers of The Home Depot of the US. In 2013, 40 million credit-card numbers were lifted from Target in the US.[5] Verizon says that the number of data breaches around the world where at least 100 million identities were exposed numbered 15 in 2016, 13 in 2015 and 11 in 2014.[6] Stolen items such as these are then traded undetected on the internet.

Cybercrime, according to some estimates, is already a US$1 trillion industry worldwide and is growing fast.[7] In the US, the FBI says that reported ransoms paid to hackers jumped from US$24 million in 2015 to US$209 million in the first three months of 2016.[8] The UK's National Crime Agency says cybercrime is underreported yet was responsible for the majority (53%) of recorded crime in the UK in 2015. The country's Office of National Statistics estimates there were 2.46 million cyber incidents in the UK in 2015 and 2.11 million victims.[9]



Source: UK's Office of National Statistics.

Whatever the true figures, identification theft, fraudulent online transfers, payment-card frauds, network assaults, denial-of-service attacks by malicious networks of computers (botnets), ransomware, cyberbullying, trolling and online child pornography are too common. They show that nothing is safe on the internet – apart from criminals, it seems. It is incredibly difficult to protect computers, networks and the internet from vandals, pranksters, criminals, terrorists, rogue governments and government-protected agents because networks are too widely used, too complex, too fragmented and too vulnerable to coding mistakes, ignorance and complacency, and too open to be defended. Governments engaged in cyberwarfare – the US military intelligence built EternalBlue – are possibly making the internet less safe. The growth in the cloud and the 'Internet of Things' – when electrical devices including cars, light bulbs and fridges become interconnected via the internet– magnify vulnerabilities. While the most likely outcome is that people will accept the crime risks of using the internet, a catastrophic attack that snaps the public's faith in cybersecurity cannot be ruled out. Europol estimates that already 85% of internet users "feel at risk of becoming a victim of cybercrime".[10]

If people, businesses, governments and other bodies including hospitals can't trust the internet to protect data, share files, host websites, seamlessly send and receive messages and make payments, an internet slowed by protections and precautions could assume a lower profile in everyday life – or fall well short of its potential anyway. But that won't happen without a fight. Policymakers are making cybersecurity a top priority while an industry has sprung up to protect cyberspace. The fight to maintain the public's trust in the security of internet will be never-ending.

To be sure, billions of interactions happen every day on the internet without hassle. A cyberattack is yet to trigger a catastrophe. Firewalls, virus antidotes and sophisticated behavioural defences help protect systems. Better protection is a key benefit of cloud computing. The payments companies, namely American Express, MasterCard, PayPal and Visa, have never suffered a significant breach, even though they are under constant attack. Neither have the big digital platforms and now the big cloud companies Amazon, Facebook, Google and Microsoft of the US and Alibaba and Baidu of China. Their growing success gives them more money to direct at security. Authorities are getting better at tracking cybercriminals. WannaCry may serve to shake people out of any complacency about cybersecurity. The core problems, though, are that the foundations of the internet are insecure and making the internet safer from criminals makes it safer for villains too – encryption software and other efforts to legitimately protect privacy are prime examples of this dilemma. Cybersecurity will be an unwinnable war that taxes society. The challenge is to keep these costs well in check so that the internet remains a massive net benefit for the world. This goal is achievable, if cybersecurity receives the priority it is due.

Fragile and flawed

Companies, governments and even people's home computers are targets for cybercriminals. So too are connected teddy bears, smart TVs and cars. Each device communicates through the internet, which is a series of networks made up of hardware and software. The internet was originally designed to connect a few trusted parties, not billions of people worldwide. Thus, the underpinnings of the networks that comprise the internet were never designed with cybercriminals in mind.

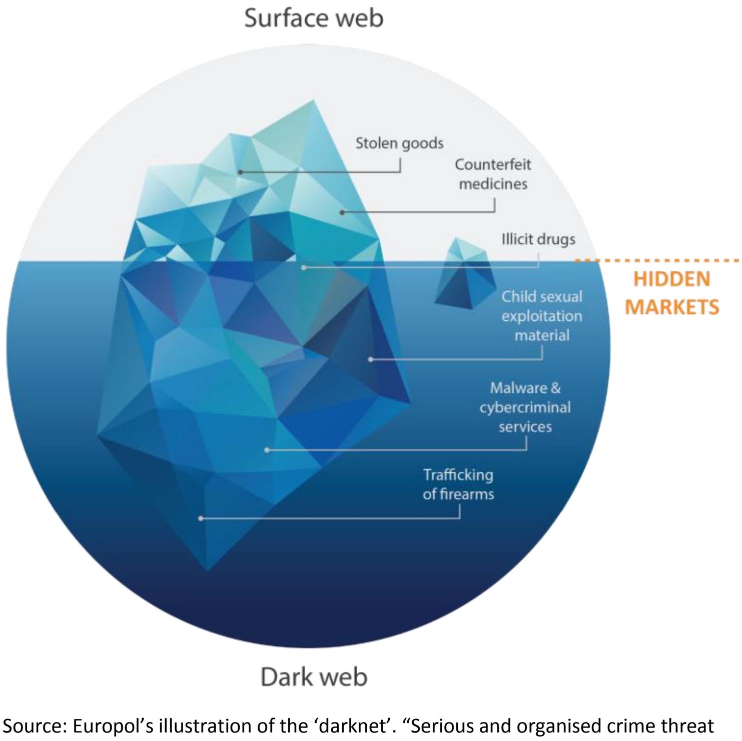
Networking hardware can offer cybercriminals a way into a network either by accident or by design. When new cutting-edge equipment is released, it is usually beyond the abilities of cybercriminals to exploit. Unfortunately, cybercriminals generally have time on their side because the expensive task of upgrading networking equipment is done sparingly by businesses. Older hardware is more vulnerable to attack. Hackers can exploit cracks in the links between different networking products from multiple companies. Finally, networking hardware companies may secretly provide 'back doors' for their governments to exploit. Criminals and others may take advantage should the government lose control of this information as happened with WannaCry. For these security reasons, the US government has banned some of its agencies from buying networking hardware from Huawei and ZTE, two major Chinese providers.[11] Cisco is similarly blacklisted by Chinese government agencies.

Software may be even more vulnerable because each application consists of millions of lines of code. All programs contain coding mistakes and inefficiencies when launched. Software makers issue 'patches' for these errors, if they find them. This takes time and effort, which often only the largest software firms can afford. Google, for example, offers regular and large cash prizes to hackers who can find vulnerabilities in the Chrome browser and operating system. Even when patches are released, many users fail to install them in a timely manner. Many people are not aware that software updates fix security flaws. Companies sometimes avoid upgrading software because the latest versions might be incompatible with bespoke applications built internally or purchased from other vendors. The outcome is that much of the internet lies unprotected. Once a software or hardware vulnerability is found and hackers seek to exploit it, to succeed, they first need to find a flaw that gives them an opening to embed into a computer some malicious digital instructions. This often doesn't require advanced computer literacy, only a knowledge of human psychology. All it can take is one person to be fooled by an innocuous-looking 'phishing' email, click on a malicious web-based ad or download from a compromised site. Odds are high this will happen because hackers bombard networks the world over every day. IBM estimates that 40% of spam emails in 2016 contained malware, up from less than 1% in 2015.[12]

Better news for honest internet users is that the cloud is relatively secure. To generate economies of scale, hyperscale public cloud vendors – Amazon Web Services, Microsoft Azure and Google Cloud Platform – are reducing the hardware and software complexity in their data centres, which makes them safer. Another boost is that these companies can spend more on security as they can spread these costs across IT investments that are multiple times the size of the largest enterprise customers. In addition, cloud applications such as Salesforce or Microsoft Office365 patch automatically and frequently, reducing the chance that user lethargy may impede protections.

Mafia-style gangs

Hackers were around in the early days of computers but perhaps many were just geeks causing trouble for kicks. Nowadays, cybercriminals operate in sophisticated packs that have management structures. These gangs run websites with drop-down crime menus, offer chat-app technical services to help would-be hackers and manage call centres to help victims pay ransoms. These felons are often protected by governments. They have access to cheap and easy-to-use tools that hack past password protections, even biometrics such as voice recognition, fingerprints[13] and iris scanning.[14] While biometrics have much promise, it has been found they too can be stolen but, unlike passwords, they cannot be reset.[15] (Using a dummy eye, the Samsung Galaxy S8 iris scanner was fooled by German hackers within a month of its 2017 launch.)[16] The internet lets criminal entrepreneurs offer what is known as 'crime as a service', a term that covers online criminal businesses that can be run by one or a handful of people.



Source: Europol's illustration of the 'darknet'. "Serious and organised crime threat assessment 2017. Crime in the age of technology."

Much criminal activity takes place on the 'darknet'. This term describes a distributed anonymous network within the 'deep web' that takes special software (TOR, I2P and Freenet) to access and is beyond the reach of authorities (and search engines). The 'darknet' is where firearms, credit-card details, child pornography, malware and cybercrime services are for sale, including to terrorists.

Cybercriminals look for undefended systems so they target charities, schools, hospitals, small businesses and households. The ransoms demanded tend to be small amounts; say one Bitcoin that was worth US$2,700 in mid-June. But it adds up. The Cyber Threat Alliance, which was formed by some Nasdaq-listed companies, claims that the 'CryptoWall Version 3' ransomware mounted 406,887 infection attempts in 2014 and plundered US$325 million from its victims.[17] Research in 2016 by the University of Kent found that 26% of ransomware victims paid the ransom and of those about 35% didn't recover anything after paying.[18]

Thanks to technological advancements that allow for mass criminal activity while protecting anonymity, cybercrime is lucrative, hard to detect and even harder to prosecute. The non-profit RAND Corporation says that "the (cybercrime) black market can be more profitable than the illegal drug trade".[19] Authorities, however, can claim some triumphs as policing is receiving more resources and technical detective work is improving. The most successful cybercrime investigation so far is probably the four-year 30-country-strong operation that in 2016 shut down an international criminal infrastructure platform known as 'Avalanche', which launched mass malware attacks that reaped millions of euros in ransoms. Authorities seized, 'sinkholed', or blocked more than 800,000 domains as part of their crackdown. Five people were arrested.[20]

Negligent users or conflicted developers?

Government and businesses are taking cybersecurity more seriously with each attack. The public expect online services that are first-class and safe. But technological advancements quickly render the best defences obsolete. Regulators see cybersecurity as a business governance issue – that directors are responsible – rather than an IT problem. They are considering forcing special disclosure of cyber risks. Businesses that fail to keep computer systems as secure as possible (by, say, not installing the latest security patches) are at risk of being sued.

To help protect networks, governments including Australia's have set up cybersecurity centres (acsc.gov.au) that pool knowledge from police, the military, academia and the private sector. An industry has sprung up to help mitigate cybercrime. Check Point Software Technologies, Cisco Systems, FireEye, Palo Alto Networks and Symantec are among the biggest listed cybersecurity companies. 'Bug hunters' are another source of internet protection. These are geeks who receive bounties from companies for finding flaws that can be fixed. Insurers are offering (partial) protection against cybercrime.

A major responsibility for keeping the internet safe, however, lies with the operating-system developers, due to their huge number of users. Microsoft Windows software is used by about 80% of the world's personal computers, Google's Android on more than 80% of the world's smartphones and Apple has the balance of both markets. Consequently, internet security falls to a large extent on these US West Coast giants.

Microsoft software products include Windows XP, the model that WannaCry exploited. As is typical for software companies, Microsoft puts a finite life on its software versions when released. In the case of Windows, it is generally 10 years, well beyond the life of a PC on which it would run. In the case of Windows XP, Microsoft provided free support for more than 12 years. Microsoft needs an 'end of life' date on software because it is costly to update and patch a software version, especially as the company is supporting a dwindling number of users who have not upgraded to newer versions. After this date, users can choose to pay to keep support alive, or they can become vulnerable. These 'end of life' dates are well flagged, as it was for Window XP when it reached its 'end of life' in 2014, almost 13 years after its launch. Despite this decades-old transparent commercial policy, Microsoft released a free patch for EternalBlue once the scale of the WannaCry attack was clear.

Despite the negligence of enterprises that still use Windows XP while refusing to pay for support after its 'end of life', in the aftermath of the WannaCry attack, Microsoft stood accused of holding back on issuing a free repair for Windows XP that could have protected users.[21] (Almost perversely, such attacks boost software and security revenue for Microsoft and its peers.) Critics suggest that Microsoft would have provided support if not for its profit motive to sell software patches, and that it has an incentive to avoid providing security updates on old software, to force people to buy the latest versions. A bugbear for many people is that companies such as Microsoft bear little or no responsibility under US law if their software is vulnerable to attack.

Expect big political fights about the liabilities of software makers in coming years as cybercrime costs mount. Stricter regulation around cybersecurity, though, could stifle innovation.

Invisible but lethal

While governments are giving greater priority to cybersecurity, the most likely catastrophic assault on the internet is by a state-sponsored cyberwarfare attack, say, by North Korea – after all, criminals have no incentive to devastate the source of their livelihood.

Western countries are especially vulnerable to a cyberwarfare attack. They depend on the computer-based global financial system. Their electric grids, emergency services, mobile communications and water services are operated by computers. Vast swathes of a country including major cities could suddenly be without power, water, the internet and emergency services. As a harbinger of the trouble that could be caused, just before midnight on April 8, hackers turned on Dallas's 156 emergency sirens, which then wailed for about 90 minutes.[22]

Western democracies engage in cyberwarfare themselves, of course. The 'Hiroshima moment' or watershed event for cyberwarfare arrived in 2010 when the US and Israel allegedly deployed the Stuxnet cyber virus to destroy centrifuges at an Iranian nuclear facility. Western spy agencies including the CIA and the UK's equivalent routinely use the internet to eavesdrop, as Wikileaks revealed this year.[23] (The CIA has found vulnerabilities in Samsung's Tizen operating system that allow it to eavesdrop via Samsung smart TVs.)[24]

Rogue governments are adept at cyberattacks. North Korea apparently hacked Sony in 2015 as revenge for an unflattering comedy about its leader Kim Jong-un, and is blamed for the theft from Bangladesh's central bank. Symantec blames WannaCry on a group from North Korea where everything is state controlled.[25] Russia staged its first notable cyberwarfare attack in 2007 when

Moscow crippled Estonian government and businesses websites for days as a warning against alleged discrimination against native Russians. In 2008, Russian hackers silenced Georgian government and media websites when Russian troops invaded the neighbouring country. More recently, Moscow took down the Ukraine electricity supply in 2016, and stands accused of interfering in the 2016 US presidential election.[26]

Other governments engage in commercial-based cyberespionage too. China's cybersecurity law of 2016 forces multinationals to store much China-gathered data in China and receive Beijing's clearance to install key hardware and software. Many Western companies think the law is designed to enable theft of their data and proprietary information.[27]

Cyberwarfare is likely to be a never-ending arms race. Democratic governments need to develop cyberwarfare technology to gather intelligence to protect their populations. The more weapons they create the more insecure adversaries feel, which prompts them to step up efforts. Another quandary is that intelligence agencies must decide whether or not to warn software manufacturers about flaws in their code. If they inform software makers (and they often do), intelligence agencies risk making worthless their cyberweaponary edge. Another conundrum is that technology companies don't like that governments develop and hold cyberweaponary, yet they have refused to co-operate when terrorists use their platforms or encryption. Underlying all this is that cyberweapon technology can be easy to steal. It can even be hard to know if a theft has taken place.

The Shadow Hackers' release of the EternalBlue malware that turned up as WannaCry is the most obvious example of stolen cyberwarfare technology ending up with villains. And this episode isn't over. Shadow Hackers has promised to release more malware stolen from US intelligence – in monthly dumps for subscribers. Web security experts warn that WannaCry will have viler successors.[28] The battle between cybercriminals and cybersecurity agents will be endless.

By Michael Collins, Investment Specialist at Magellan.

[1] Brad Smith, Microsoft president and chief legal officer, confirmed the theft of the tools from the National Security Agency in a blog on May 14 "The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack." blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#Hq24Z7FcxudfxHJX.99

[2] WannaCry spread through port 445. Computer connections have 1,024 ports to manage communications.

[3] Reuters. "Senator McCain says Russia must pay price for hacking." 30 December 2016. http://www.reuters.com/article/us-usa-russia-cyber-mccain-idUSKBN14J1LW

[4] WIRED. "That insane, $81m Bangladesh Bank heist? Here's what we know." 17 May 2016. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

[5] Bloomberg. "Missed alarms and 40 million stolen credit card numbers: How Target blew it." 18 March 2014. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data

[6] Verizon. "2017 Verizon Data Breach Investigations Report". www.verizonenterprise.com/Verizon-insights-lab/dbir/2017

[7] Lawrence Miller, certified information security systems professional. "Advanced endpoint production for dummies." Palo Alto Networks special edition. John Wiley & Sons. 2015. Page 3.

[8] Reuters. "Ransomware: Extortionist hackers borrow customer-service tactics." 12 April 2016. http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X. FBI. "Ransom victims urged to report infections to federal law enforcement." 15 September 2016. https://www.ic3.gov/media/2016/160915.aspx

[9] National Crime Agency. "Cyber crime assessment 2016." 7 July 2016. Version 1.2. Page 6. http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

[10] Europol. "Serious and organised crime threat assessment. Crime in the age of technology." Page 29 of printed version. https://www.europol.europa.eu/socta/2017/

[11] Techonomy.com. "Huawei, ZTE banned from selling to US government." 2 April 2013. http://techonomy.com/2013/04/huawei-zte-banned-from-selling-to-u-s-government/

[12] IBM report. "Ransomware: How consumers and businesses value their data." 2017. Page 4. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03135USEN&

[13] WIRED. "The trouble with Apple's touch IDS fingerprint reader." 3 March 2013. https://www.wired.com/2013/12/touch-id-issues-and-fixes/

[14] Forbes. "Hacking Putin's eyes: How to bypass biometrics the cheap and dirty way with Google images." 5 March 2015. https://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/#14d21ab9214a

[15] Yahoo! Tech. "The 2 big problems with fingerprint security." 29 January 2015. https://www.yahoo.com/tech/the-2-big-problems-with-fingerprint-security-109371608679.html

[16] Guardian. "Samsung Galaxy S8 iris scanner fooled by German hackers." 23 May 2017. https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security. To see the video of how it was done, go to: https://media.ccc.de/v/biometrie-s8-iris-en

[17] Cyber Threat Alliance. Cyber Threat Alliance cracks the code on Cryptowall crimeware associated with $325 million in payments." 29 October 2015. https://cyberthreatalliance.org/pr/pr-102915.html

[18] University of Kent. "2016 Kent cyber security survey." The survey was conducted online from 5 to 8 August 2016. https://cyber.kent.ac.uk/Survey2016.pdf

[19] RAND National Security Research Division. "Markets for cybercrime tools and stolen data. Hacker's bazaar." 2014. Page ix. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

[20] Europol. "'Avalanche' network dismantled in international cyber operation." 1 December 2016.

https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

[21] Financial Times. “Microsoft held back free patch that could have slowed WannaCry attack.” https://www.ft.com/content/e2786cbe-3a97-11e7-821a-6027b8a20f23. (Subscription needed.)

[22] Dallas News. “Hacking blamed for emergency sirens blaring across Dallas early Saturday.” 8 April 2017. https://www.dallasnews.com/news/dallas/2017/04/08/emergency-sirens-blare-across-dallas-county-despite-clear-weather

[23] WIRED. “Wikileaks just dumped a mega-trove of CIA hacking secrets.” 7 March 2017. https://www.wired.com/2017/03/wikileaks-cia-hacks-dump/

[24] The Verge. Samsung’s TV and watch OS is reportedly full of security holes.” 4 April 2017. https://www.theverge.com/2017/4/4/15175124/samsung-tizen-security-vulnerabilities-issues-flaws

[25] New York Times. “More evidence points to North Korea in ransomware attack.” 22 May 2017. https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html?ref=business

[26] Newsweek. “Inside Putin’s campaign to destroy US democracy.” 18 May 2017. http://www.newsweek.com/2017/05/26/inside-putin-campaign-destroy-us-democracy-610401.html

[27] The Economist. “The noose tightens. China adopts a tough cybersecurity law. Foreign firms are worried.” 10 November 2016. http://www.economist.com/news/china/21710001-foreign-firms-are-worried-china-adopts-tough-cyber-security-law

[28] Fortune. “Meet EternalRocks, WannaCry’s scarier successor.” 22 May 2017. http://fortune.com/2017/05/21/wannacry-successor-eternalrocks/?xid=newsletter-brief

Important Information:

This material has been prepared for general information purposes and must not be construed as investment advice. This material does not constitute an offer or inducement to engage in an investment activity nor does it form part of any offer or invitation to purchase, sell or subscribe for in interests in any type of investment product or service. This material does not take into account your investment objectives, financial situation or particular needs. You should read and consider any relevant offer documentation applicable to any investment product or service and consider obtaining professional investment advice tailored to your specific circumstances before making any investment decision. This material and the information contained within it may not be reproduced or disclosed, in whole or in part, without the prior written consent of Magellan Asset Management Limited. Any trademarks, logos, and service marks contained herein may be the registered and unregistered trademarks of their respective owners. Nothing contained herein should be construed as granting by implication, or otherwise, any licence or right to use any trademark displayed without the written permission of the owner. No part of this material may be reproduced or disclosed, in whole or in part, without the prior written consent of Magellan Asset Management Limited.