Avoiding ‘cybergeddon’: ESG risk in an interconnected world

Sumant Wahi
Senior equity analyst

Jonathan Tseng
Senior equity analyst

Mike Morey
Equity research analyst

Mendy Zhang
Equity research associate

Ronald Chung
Investment analyst

Federico Wynne
Senior Credit analyst

Raji Menon
Investment writer

Cybersecurity and data protection are rapidly emerging as some of the biggest environmental, social and governance (ESG) risks for companies to manage. Demographics and record debt, along with technological change, however, do not leave monetary authorities much room to act aggressively in a globally coordinated way.

Fidelity’s 2018 Analyst Survey shows they are one of the top concerns for companies and indicates their increased spending on technology as they race to strengthen their defences. The World Economic Forum’s Global Risk Report ranks both large-scale cyberattacks and major data breaches as the third and fourth biggest global risk for 2018 - the highest in the history of the report - just behind extreme weather conditions and natural disasters.

Spending projections reveal the size of these threats. Global cybersecurity spending is expected to top $1 trillion (cumulatively) by 2021, while the costs of cybercrime are likely to soar to $6 trillion by 2021, up from $400 billion in 2015.[1]

Reputational damage, legal costs and potential data losses can undermine a company’s profitability or even threaten its very existence. This is why assessing a company’s cyber risks is critical to any equity or bond investment decision.

Rise of cloud solutions

Where many see risks, some see opportunities. One of the fastest-growing areas in information technology is cloud computing, which allows clients to store and manage data on remote servers rather than on local servers or on site. This space is dominated by the three US technology giants Amazon, Google and Microsoft.

Cloud applications offer cost savings and flexibility, because only the most critical or sensitive data needs to be kept on site. For example, the British retailer River Island, which moved its website to Amazon’s cloud recently, said it could now boost capacity during peak periods like the Black Friday sales in November, and added that hosting the site on the cloud made it cheaper and easier to experiment with new ideas in digital retailing.

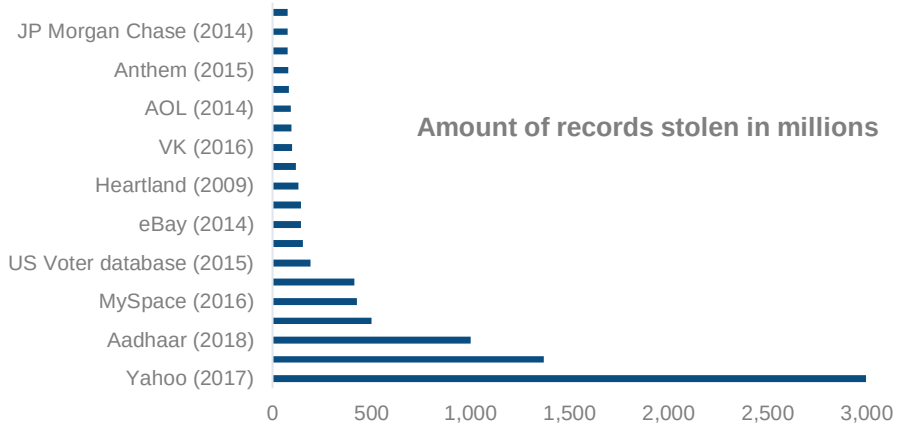
But as the number of companies which transfer data to one of the big three providers grow, data security becomes more pressing. Hosting data with cloud service providers is generally seen as safer than keeping data in-house, due to the quality of the big three’s security processes, the expertise of their staff and the ongoing investment in their services. The downside is that a hack could potentially expose client data on unprecedented levels.

A growing number of small third-party providers are jumping into the fray to offer additional layers of security to clients who use the big three’s services but are keen to enhance their security features. Check Point Software, Palo Alto Networks, and Zscaler (which made its initial public offering in March 2018) are all examples of such add-on security providers.

Commoditisation of cybercrime

In 2017, Yahoo revealed that every one of its three billion accounts was affected by a data theft in 2013, while the 'WannaCry's' ransomware attacks crippled Spain's Telefonica, American courier service FedEx and large parts of the UK's National Health Service.

Chart 1: Rising trend of cyberattacks on companies



Source: Statista, February 2018

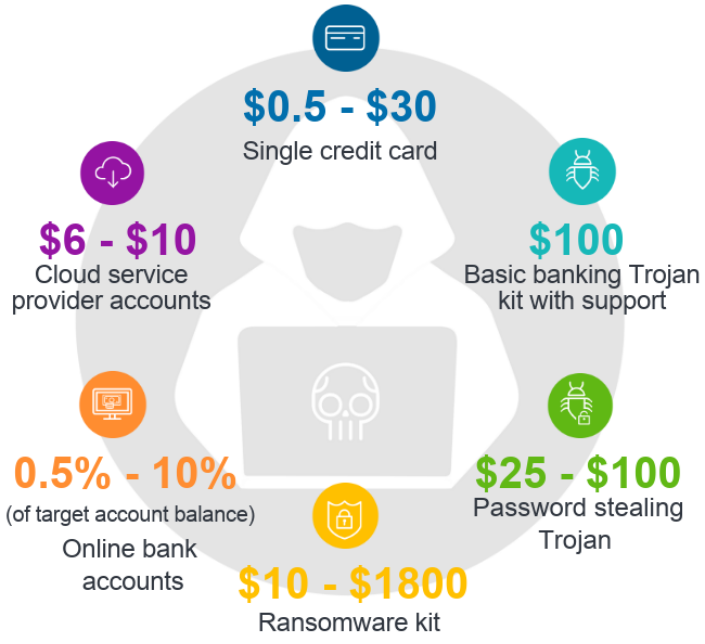
https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

Cybercrime was once the preserve of backroom nerds or skilled gangs but has now become commoditised on a large scale. 'Exploit kits' are readily available on the black market, making it far simpler and cheaper for cybercriminals to carry out attacks.

A ransomware toolkit can be bought on the dark web for as little as $10 fueling the surge in attacks of the likes of 'WannaCry', 'Petya' and 'Not Petya'. Ransomware is a type of software that encrypts a victim's data and threatens to publish or permanently block access to it unless a ransom is paid.

While small and medium businesses did not have to worry about this kind of malware previously, the simplification and accessibility of cybercrime have forced many of them to adopt improved security features. Cloud-based service providers which offer low-cost solutions and flexibility have been significant beneficiaries of new business from these small and medium sized firms.

Graph 1: Cybercriminals no longer need large budgets



Source: Symantec Internet Security Threat Report 2017

Regulators take a tough stance on privacy

The dominance of the US technology giants, not just in cloud solutions, has prompted a wave of regulatory guidance on issues ranging from monopoly and taxation to net neutrality. Privacy of personal data is another area of growing concern for regulators both in Europe and the US.

The latest salvo by the European Union comes in the form of its General Data Protection Regulation (GDPR) which takes effect in May 2018. The directive aims to strengthen data protection for EU citizens by setting rigorous timelines for businesses to report data breaches and enshrining the 'right to be forgotten'.

Despite the regulator's best intentions, GDPR may end up strengthening Google and Facebook by forcing businesses to avoid the bureaucratic hassle around GDPR rules altogether and instead opt to reach customers through the tech giants. The British pub chain J D Wetherspoon, for example, announced last year that it would delete its entire email mailing list and said customers could instead follow the company on Twitter and Facebook.

Data protection, however, doesn't end with measures like GDPR. The sheer reach of these platforms is worrying policy makers enough to take further action. Their next target may be Facebook over its role in creating 'fake news' and influencing voter behaviour in the 2016 US presidential election and the UK's 'Brexit' referendum. Some 126 million US users viewed political advertisements placed directly or indirectly by Russian agencies on Facebook at the time, foreign interference on a scale well beyond most voters' wildest imaginations.[2]

Facebook has also come under fire for allowing a firm linked to Donald Trump's campaign team to exploit the private information of 50 million users.[3] Facebook shares have nosedived and CEO Mark Zuckerberg has been forced to apologise for the firm's role in the data breach. The issue of whether Facebook is a media company or a data analysis company - and what checks are required - is one that regulators are considering as a matter of some urgency. Social media intervention now poses a credible threat to sovereignty and/or democracy. Investors' worries over the looming threat of increased regulation for the tech giants triggered a steep fall in share prices in the last week of March.

China-bound

Technology firms' dominance and personal data privacy is not just an issue in the US. China's internet giants, often called the 'BATs' - Baidu, Alibaba and Tencent - are coming under increasing investor scrutiny for their relationship with the Chinese authorities.

Executive teams in these companies work closely with the Chinese government to ensure compliance, and are required to make investments in non-tech sectors where return on investment is generally considered low. The government also plans to pick up stakes in some of these companies. Such stakes are expected to come at a discount and could potentially affect commercial decisions, adding to the costs of doing business in China.

The BATs may be more used to government involvement but for foreign firms some demands can be unpalatable. A tough new cybersecurity law, for example, requires local and overseas firms to submit to security checks and store user data within the country. This data can, in theory, be passed on to the Chinese government if they make a request for such information.

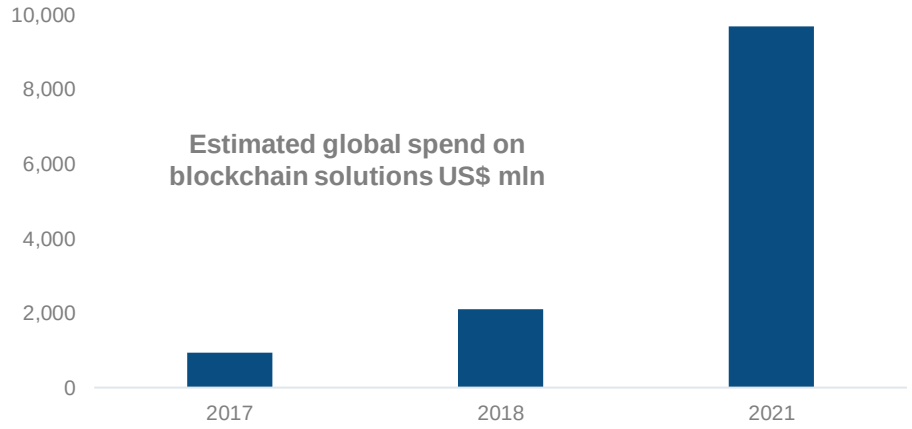
Chinese users are also becoming increasingly sensitive to how their personal information is handled by the tech giants. Earlier this year, Ant Financial, Alibaba's payments affiliate, was forced to apologise for making the opt-in to its social credit scoring service the default when users opened a new report in the app.

Blockchain: Transforming ESG through technology

While technology can increase risks, it can also strengthen ESG standards through applications like blockchain. Behind the noise around bitcoin, the technology underpinning it - blockchain - is quietly improving the transparency of supply chains in myriad areas: from seafood and tea to conflict minerals and blood diamonds.

A new International Data Corporation report estimates that global spending on blockchain solutions is expected to reach $2.1 billion in 2018, more than double the $945 million spent in 2017. Over a five-year period to 2021, total spend is expected to rise to $9.7 billion.

Chart 2: Global Spending on blockchain solutions



Source: International Data Corporation, January 2018

Blockchain is a distributed ledger technology; it uses digital encryption to create an immutable, transparent history of product authenticity and ownership. Earlier this year, Maersk said it was working with IBM to digitise its supply chains, while a group of the world's largest retailers and food companies including Nestle, Walmart and Unilever said they would work with IBM to explore how blockchain technology could be used to improve food traceability by providing trusted information on the origin and state of food. Blockchain is also being used to increase traceability and prevent fraud in the seafood industry.

Everledger, a startup which initially started using blockchain to track diamonds, has now expanded its use to coloured gemstones, jewellery, fine wine and art. By creating a global registry for diamonds, the risk of counterfeit, insurance fraud and smuggling from conflict zones can be significantly reduced.

This technology is not just being harnessed by companies; Sierra Leone became the first country in the world to use blockchain to tally election votes in a move that could reduce or eliminate vote count rigging. Such a move could prove a boon for institutional investors in frontier markets. Honduras, meanwhile, is testing the use of blockchain to build a land title registry that will help reduce land title fraud, a common issue in poorer countries.

But there could be risks around the use of blockchain. For example, blockchain's immutable transaction history could be at odds with the EU's General Data Protection Regulation 'right to be forgotten' rule. According to Sustainalytics, an ESG research and ratings provider, the energy required to power the computers which operate blockchain is also an area of potential concern. Depending on implementation, the technology could need a number of servers and data centres to function, which can be energy intensive.

The growing complexity of cyberattacks means that companies will have to spend more on shoring up their defences. The unprecedented growth in cybersecurity seen in recent years looks set to continue, with newer providers offering top-ups to existing cover.

Investors need to consider the impact of a cyberattack in any potential investment decision.

Technology can wreak havoc on a company's prospects, but advances in the form of blockchain can also be a force for good, transforming ESG through transparency and human rights management.

Technology is ever more powerful but not always to be feared.

References

1] https://cybersecurityventures.com/cybersecurity-market-report/

2] https://www.reuters.com/article/us-usa-trump-russia-socialmedia/facebook-says-126-million-americans-may-have-seen-russia-linked-political-posts-idUSKBN1CZ2OI

3] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election