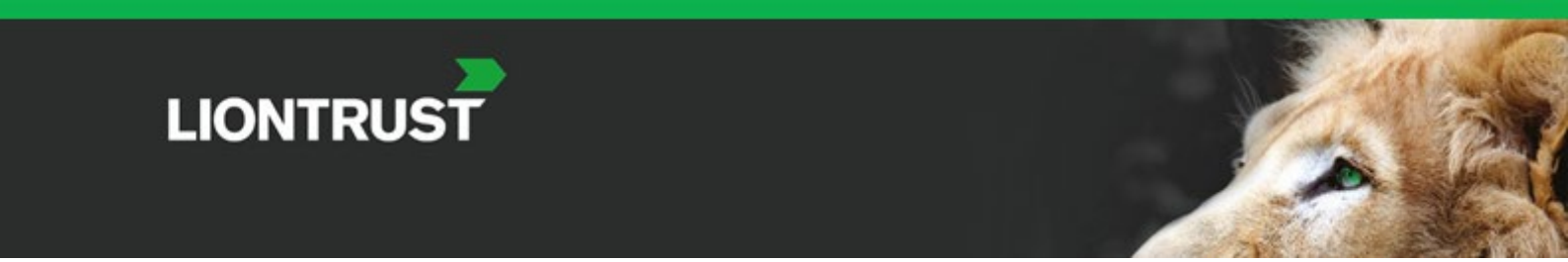

Cybersecurity – new-age challenges and threats

As the world grows increasingly digital, we are simultaneously seeing an increase in the frequency, severity, and inventiveness of cyber-attacks. Digital databases are growing, and can be lucrative targets for criminal actors, with significant financial – and more real-world – implications for targets and stakeholders. From an investment perspective, the evolving, contrasting landscape of digital opportunity and cyber threat provides an array of opportunities and challenges.

As we emerge into a post-Covid world, it is evident that the businesses best positioned to continue to take advantage of the drive to digitisation are not only the most innovative and technologically advanced, but those with access to sizable digital assets and databases which can be leveraged to enormous value.

However, every rose has its thorn: the accelerating digital shift and escalating data harvest means companies are also becoming more exposed to a variety of new-age challenges and threats.

The maths is simple – the increasing prominence of digital assets, technologies, and databases mean individuals, businesses, and governments are becoming increasingly exposed to criminal cyber security threats which are evolving Pari Passu with cyber-security defences.

James O'Connor, Deputy Manager of the Liontrust Income Fund, says: "Digital hacks, leaks, and breaches can have significant financial, operational, reputational, and more "real-world" consequences for not only the intended targets, but also for stakeholders such as customers, staff, constituents, shareholders, suppliers, communities, and governments."

O'Connor also highlights that heightened geopolitical tensions serve to add fuel to the fire as state-sponsored bad actors are increasingly deployed in attempts to disrupt and destabilise public and private targets as a form of covert warfare; this is reflected in political discourse and the increased allocation of defence spending towards areas such as electronic systems and cyber defence.

"Even in the case of a slowdown in Russia/Ukraine war activity, management teams we have met with express concern that this will result in an increase in bad-actors shifting attention back to the corporate market."

While public sector targets may be desirable for state-sponsored disruption, private businesses are often more lucrative quarry for criminal actors, and the digital evolution is in part to blame – avenues of exposure are growing, accelerated by a confluence of factors such as the shift to remote working (more potential attack points), increasingly complex supply chains (less line-of-sight on exposure), the transition to cloud computing (more data stored off-premise), and the digitisation of previously analogue operations and services (more parts of a business can be disrupted).

Some businesses are more at risk than others. Companies with poorly integrated, under-invested, or legacy systems are low-hanging fruit, as digital defences are more readily breached. Companies with

significant digital datasets – particularly sensitive personal customer data – are lucrative targets for activities such as phishing, as extracted information can be sold or exploited to enormous value. Meanwhile, businesses that are highly sensitive to operational disruption are more susceptible to ransomware attacks, as the cost of operational delays can outweigh the ransom demanded from criminals holding their operations hostage.

One need only open a newspaper to see FTSE-listed companies continue to suffer from breaches of varying severity. Recent examples include **Royal Mail Group**, **WH Smith**, **Reckitts, WPP, Vesuvius**, **Morgan Advanced Materials**, **Intercontinental Hotels Group**, **Genuit**, **JD Sports**, and **Weir**.

Investment challenges arise from both sides of the equation. In terms of digital opportunity: companies that lag peers in terms of digital technologies, appropriate skills (e.g., tech-savvy staff and management), or access to databases will either need to invest to play catch-up or cede ground to competitors and new disruptive challengers, posing risks to both competitive positioning and earnings growth.

From a cyber-threat perspective: companies that have outdated or poorly integrated legacy systems, have vast amounts of personal customer data, or are highly sensitive to disruption are lucrative targets for criminals and thus at higher risk of an attack. These breaches can have significant financial, operational, reputational, and regulatory repercussions for companies and stakeholders. Put simply, strong cyber-security management is a must-have to mitigate these risks.

On balance, this dynamic structural backdrop serves to highlight the importance of engagement as a key part of company analysis. O'Connor adds: "As investors, we engage with hundreds of companies every year through one-one-one meetings, conferences, and company and industry events; this level of engagement not only allows us to probe any key issues that we have identified in our analysis, but also helps us to understand management's thinking process and business insights in a way that is difficult to replicate through other means."

"Direct interactions with management allow us to paint a clearer picture on this front, and we are increasingly using this channel to ensure that management are well invested to capture digital opportunities and manage the ever changing cyber threats that may lie ahead."

For more insights and views from Liontrust visit: https://www.liontrust.co.uk/insights/ourinsights

For a comprehensive list of common financial words and terms, see our glossary at: https://www.liontrust.co.uk/glossary

move significantly, this may have a notable effect on the value of that portfolio. Investment in the funds may involve foreign currencies and may be subject to fluctuations in value due to movements in exchange rates.

Some of the funds may invest in emerging markets/soft currencies and in financial derivative instruments, both of which may have the effect of increasing volatility.

Disclaimer

This communication is issued by Liontrust Fund Partners LLP (2 Savoy Court, London WC2R 0EZ), authorised and regulated in the UK by the Financial Conduct Authority (FRN 518165) to undertake regulated investment business.

This is a marketing communication. Before making an investment, you should read the relevant Articles of Association and the Key Investor Information Document (KIID), which provide full product details including investment charges and risks. These documents can be obtained, free of charge, from www.liontrust.co.uk or direct from Liontrust. Always research your own investments and if you are not a professional investor please consult a regulated financial adviser regarding the suitability of such an investment for you and your personal circumstances.

This should not be construed as advice for investment in any product or security mentioned, an offer to buy or sell units/shares of Funds mentioned, or a solicitation to purchase securities in any company or investment product. Examples of stocks are provided for general information only to demonstrate our investment philosophy. The investment being promoted is for shares in a company, not directly in the underlying assets. It contains information and analysis that is believed to be accurate at the time of publication, but is subject to change without notice. Whilst care has been taken in compiling the content of this document, no representation or warranty, express or implied, is made by Liontrust as to its accuracy or completeness, including for external sources (which may have been used) which have not been verified. It should not be copied, forwarded, reproduced, divulged or otherwise distributed in any form whether by way of fax, email, oral or otherwise, in whole or in part without the express and prior written consent of Liontrust. [23/186]