17 96

LOMBARD ODIER
INVESTMENT MANAGERS

Cybersecurity in the FinTech sector:
A regression analysis on the impact of cyberbreaches on company fundamentals

– For professional investor use only –

03/23

March 2023

The market is currently inefficient in pricing how a cyberbreach impacts company fundamentals

p.03

Hacked companies disclose higher capital and operating expeditures as a direct result of having to restore the operational and brand damage caused by the attack versus non-breached peers

This document has been prepared by:

Jeroen van Oerle
Portfolio Manager

Foort Hamelink
Senior Solutions Manager

Charlie Parker-Williams
Quantitative Analyst

For further information please visit www.loim.com

Introduction

In our first white paper on cybersecurity risk, we described the impact of cyberbreaches on companies, and explained a methodology to incorporate this factor into the portfolio management process.[1]

We concluded that the global average costs incurred by a data breach have increased in recent years and accelerated during the pandemic. This was the result of less-secure work-from-home environments that were installed rapidly by companies to continue operating during lockdowns, plus a steep increase in cybercrime.

We also explained our methodology for evidence-based testing on basic cybersecurity hygiene. In cooperation with one of our technology partners, we created a traffic-light procedure to translate highly technical data into ready-to-consume output for equity portfolio managers and analysts.

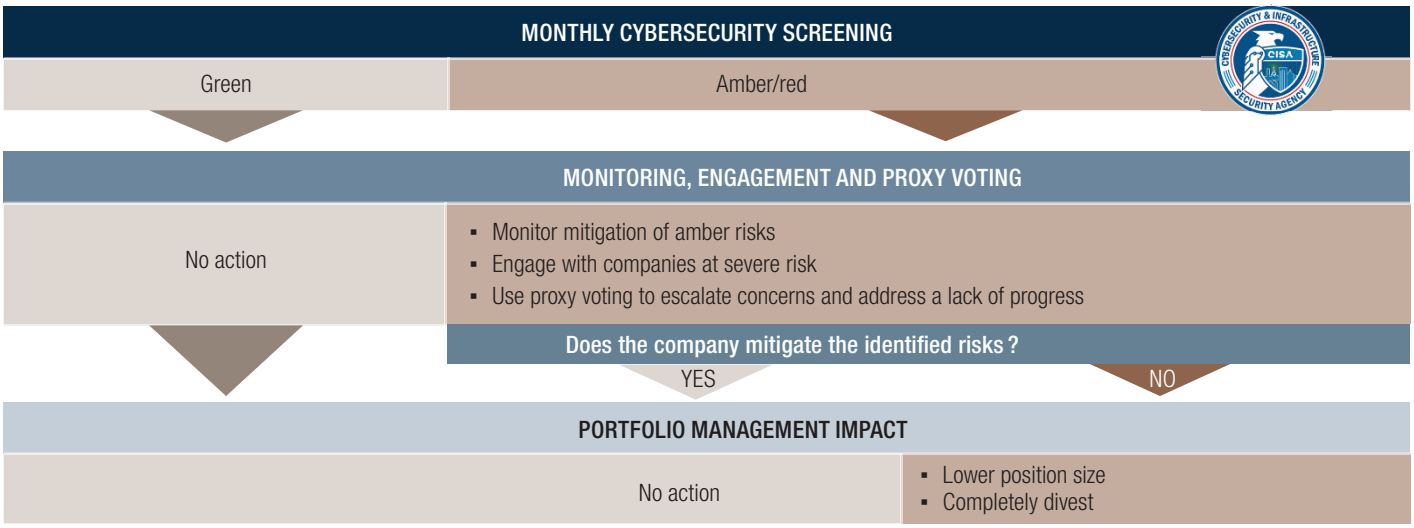
The system screens known exploited vulnerabilities in software as disclosed by the US Cybersecurity and Infrastructure Security Agency (CISA). Based on the results, we engage with companies judged to be at severe risk, so these companies can patch their software vulnerabilities and improve the risk profile of our holdings (see figure 1).

Most investors seem to agree on the importance of incorporating cybersecurity risks into the portfolio management process. However, our statistical research shows that the market, in general, does not take this factor into account when pricing assets.

We analysed a dataset by RiskRecon, a specialist in continuous vendor monitoring, which contains a list of breached companies and the date these breaches were made public. In a perfect world, assuming efficient markets, the impact of hacks on the fundamentals of involved companies would be analysed and priced in. This impact can range from increased costs incurred by countermeasures taken to prevent another hack to managing revenue implications due to a loss of trust from customers.

Since 2023, we can add regulatory fines to that list as well, especially for companies operating critical infrastructure in sectors ranging from banking to health, data, energy and defence. However, we found no statistical relationship between hacked companies and their share-price performance in an event study around the public announcement of the hack. In other words, the market does not respond to a cyber breach.

FIG. 1 LOIM GLOBAL FINTECH: CYBERSECURITY METHODOLOGY



Source: LOIM as at 2023.

[1] van Oerle, J. and Coriat, R. July 2022, "Cybersecurity: a neglected risk in a digitalised world". Published by LOIM.

Previous research has been inconclusive on this topic. In studies by Tosun,[2] and Corbet and Gurdgiev,[3] a small but significant trading effect was found on the day a hack was publicised, spurring higher bid-ask spreads and greater volatility. In another study, such as that by Rosati et.al, those effects were negligible.[4]

This inconsistency between our statistical findings and those of previous research, in combination with the lack of a link to fundamentals, caught our attention. We decided to test if the market's response to a breach was either valid or flawed. If *valid*, there is indeed no effect on the breached company's fundamentals versus its non-breached peers. If *flawed*, the market is failing to appraise the impact of a hack on fundamentals. To test which outcome is correct, we tested the effect of a breach on both the hacked company's returns and fundamentals.

Our statistical evidence supports the *flawed* hypothesis. Breached companies show a significant increase in costs compared to non-breached peers, resulting in two significant implications:

1. The market is currently inefficient in pricing how a cyberbreach impacts company fundamentals
2. Given that we show statistical evidence of impacted fundamentals, changes in prices happen at a lag because the actual out- or underperformance of a company during the quarter is being translated to the share price. This implies that investors who can assess the impact on fundamentals and respond accordingly have an edge over those who cannot

In this white paper, we describe our data and methodology, and we go deeper into our findings. We show that current measurements of cybersecurity risk via the well-known ESG-data providers are ineffective, and we propose an enhanced, evidence-based approach to integrating basic cyber-hygiene factors into the risk-management process.

[2] Tosun, O.K., 2021. "Cyber-attacks and stock market activity". *International Review of Financial Analysis*, 76, p.101795.

[3] Corbet, S. and Gurdgiev, C., 2019. "What the hack: Systematic risk contagion from cyber events". *International Review of Financial Analysis*, 65, p.101386.

[4] Rosati, P., Cummins, M., Deeney, P., Gogolin, F., Van der Werff, L. and Lynn, T., 2017. "The effect of data breach announcements beyond the stock price: Empirical evidence on market activity". *International Review of Financial Analysis*, 49, pp.146-154.

Data and methodology

Dataset

We use a sample of 81 breaches for a concentrated group of 75 fintech companies, compiled by RiskRecon over the period 2005-2022. The largest number of breaches happened between 2014-2019, as can be seen in figure 2. The companies analysed are well-established fintech names which have existed for many years. In general, the dataset can be considered a quality-growth subsection of the fintech universe and excludes hypergrowth companies with short histories.

This can potentially influence our research, because we expect companies that are fully focused on hypergrowth, in general, to pay less attention to cybersecurity. We also think that investors in hypergrowth companies are likely to have priorities other than cybersecurity, with a focus on new products being rolled out in new markets to sustain the high growth rate.

Given the companies we analysed in this sample have had their main products available in mature end-markets for some time, we are confident these businesses prioritise cybersecurity in their operations. The stability of the end-markets (and peer group) also leads to results that are more robust. Digital services and the protection of critical data should be at the core of their business activities.

FIG. 2 DATASET OF BREACHES

Year	Number of br	Percentage	Year	Number of br	Percentage
2005	1	1.2%	2014	6	7.4%
2006	1	1.2%	2015	6	7.4%
2007	3	3.7%	2016	8	9.9%
2008	1	1.2%	2017	6	7.4%
2009	3	3.7%	2018	8	9.9%
2010	1	1.2%	2019	11	13.6%
2011	3	3.7%	2020	2	2.5%
2012	6	7.4%	2021	3	3.7%
2013	8	9.9%	2022	4	4.9%
			Total	**81**	**100.0%**

Source: RiskRecon, 2023.

Methodology

We analyse the dataset by applying several statistical techniques in a methodology with three stages: share-price analysis, fundamental analysis, and an analysis of regressions on the fundamentals. We explain each stage below.

1) Share price analysis. We perform event studies to test the impact of breaches on stock-market returns. To do this, we convert the share-price data from compounded returns to month-to-month percentage changes in order to coincide with the breach dataset numbers. Next, we control for outliers by removing 2.5% of the extreme observations at both ends. We then calculate the abnormal returns of each of the hacked companies (after correcting for their market betas) and centre those around the event month (T=0). We then look at the cumulated geometric means, standard deviations and corresponding t-statistics and p-values across each of the points in time from T-6 to T+6 see if there are statistically significant differences between hacked companies and their non-hacked peers.

2) Fundamental analysis. We assess the impact on hacked companies by analysing their fundamentals in the first and second quarters after the hack, as well as in their first full-year results. We use the non-breached peer group as a proxy for normalised results, as well as the company's own earnings history and the total aggregate MSCI ACWI reference set. The peer group is drawn from the second tier of GICS, thereby consisting of companies from the same industry group as the breached firm.

We then use simple regression analysis to test a set of fundamentals to see if they significantly differ from those of peers. The Worldscope variables we apply are: capital expenditures (capex), operating expenses (opex), Selling, General and Administrative expenses (SG&A) and Sales (net sales or revenues).

Fines are not considered, because they are not part of operational costs and cannot be deducted for tax reasons. Fines resulting from hacks are difficult to separate from other fines, as they are usually not disclosed by companies, so we would have to assume that these costs add to what we identify in this study.

If cyber-breaches have no impact on fundamentals, we should find no significantly different results for quarterly and annual results for these variables when compared to their peer group and their own historic trend. (A full set of the seven different metrics across each of the balance sheet fields can be found in appendix 1.)

There are two important factors affecting the results of these regressions. First, the sample set is small, which reduces the significance of the observations. Secondly, the hacks in our sample set are compared to a sample of peers (both sector and MSCI ACWI) for which we have no data, but where we can assume the number of breaches to be larger than zero. This implies that we compare averages of our hacked companies with averages from a peer group which has also suffered hacks, which could potentially weaken the significance of our findings.

3) Regressions analysis. The third test we perform employs the so-called Lasso regression, a form of regression analysis that also incorporates regularisation functionality by shrinking or removing non-relevant features.

Especially in a case where there is collinearity (which is present in our data sample because the variables are highly correlated), this technique allows for better statistical conclusions because it filters out the correlation effects. In this LASSO regression, we use other proxies to explain the difference in the testing variables observed versus peers, such as size, country, type of hack and sustainability ratings in questionnaire-based reports from large sustainability report providers.

We then sample 80 different penalty terms from 0.01 to 0.2 (the lambda) and use an optimiser function to select the best penalty term. A lambda equal to zero would imply no penalty, hence all variables can be added to the regression, whereas an infinite lambda would imply no features can be considered. We judge whether the findings are robust when adding other explanatory variables to be sure that the results we find can indeed be attributed to the breach itself, and not to other factors. We then observe which coefficient across differencing types have p-values that indicate a statistically significant result.

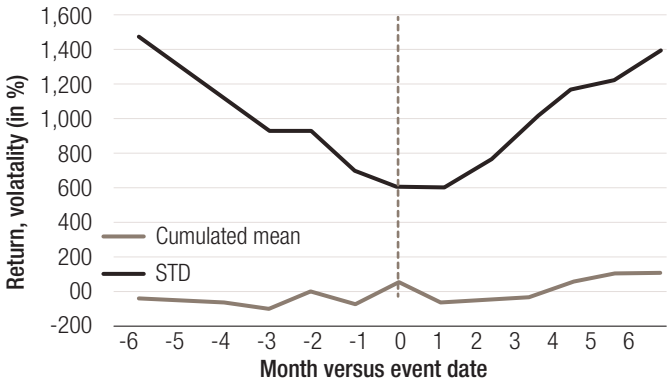
Results

1) Share price analysis

As shown in figure 3, abnormal cumulated returns in the event of a breach do not differ significantly from months without hacks. Especially considering the high rate of volatility in monthly returns, it would be very difficult to find statistically significant results in such a data set.

FIG 3. EXCESS RETURN EVENT STUDY AROUND HACK DATA, AT T=0

COMULATED RETURN AND VOLATILITY AROUND EVENT DATE



Source: LOIM, March 2023.

This differs from the work of Tosun, Corbet and Gurdgiev, who do find a significant effect in both spread and the volatility in the event of a breach versus other trading days. However, here too, there is no direct measurement of effects on prices but rather a focus on the change in volatility.

In our view, what this tells us is that a breach spurs the market to reassess the risk of the stock affected but does not actually discount the potential impact on company fundamentals in the price itself. In other words, traders notice something is going on – hence the increase in trading volume and risk – but they don't know exactly how to price that impact.

Our thesis is that this is the result of a mismatch between technical knowledge and financial expertise. If market participants had both, they could make a fair assessment of the materiality of the breach and use this to reprice the stock. In fact, if a price effect does occur, it is usually the result of the estimated impact on legal grounds (typically settlement claims with people whose data was stolen) rather than a reassessment on a company's fundamentals to reflect the increased costs in marketing and sales activity to restore the damage to reputation and margins.

There are several cases in which major breaches were followed by large share-price impacts:[5] Ebay suffered a -10% slump in 2014, Equifax fell -35% in 2017 and Twitter lost -30% in 2018. These moves made headlines, but many other breaches go unnoticed, which is evident from the data. What makes this exercise especially difficult is that the effects differ substantially by industry and type of company.

This is because the impact of cyber-breaches on fundamentals must be understood, in addition to estimated impacts of other direct consequences, like regulatory fines and legal costs.
One aspect about the breaches that we can confirm, as strange as it might sound, is that the loss of sensitive data itself is not a good measure to assess the impact on the company's stock price.
This is evident from the comparison of three of the largest breaches in history, where data of a similar nature was stolen:

The Equifax breach in 2017 affected 148 million people whose names, home addresses, phone numbers, social security data and driver's license numbers stolen. The stock price reaction was a severe -35% cratering. In contrast, when Marriott announced in 2018 that it was hacked in an attack dating back to a 2014 breach at Starwood, which was later acquired by Marriott, impacting the data of more than 500 mn guests, there was not a notable price impact. Similarly, First American Financial Corporation lost records due to a data leak in May 2019, in which 885 mn customers were affected and data concerning bank accounts, social security numbers, wire transactions and mortgages were compromised. Losses on the stock, in this case, amounted to a mere 6%. This might serve as evidence that the market differentiates between a hack and a leak, but most importantly, it shows that there are legal, regulatory and technical differences that need to be taken into account, and not so much the loss of sensible data itself.

In the next section, we assess the impact on fundamentals to understand whether the market reactions described above are fair judgements on the actual impact of a hack on a company's costs, or whether the muted stock-price movements represent a failure to properly assess how breaches impact fundamentals.

[5] Any reference to a specific company or security does not constitute a recommendation to buy, sell, hold or directly invest in the company or securities. It should not be assumed that the recommendations made in the future will be profitable or will equal the performance of the securities discussed in this document.

2) Fundamental analysis

In our first set of fundamental analyses, we test the hypothesis that there is a statistically significant effect other than zero for a company that has been hacked versus a set of benchmarks. These benchmarks can be the difference between the company's performance relative to: a) its own history (_diff_yoy_hist); b) its peer-group history (_diff_yoy_hist_sector); or c) the entire MSCI dataset history (_diff_yoy_hist_overall).

In all these events, we looked at the differences versus a three-year average. We also assessed the difference at the event period in isolation on both a year-on-year (yoy) and quarter-on-quarter (qoq) basis. The benchmarks used here are the differences relative to the sector (_diff_xxx_sector) and the MSCI universe (_diff_xxx_overall). All these variables are tested at the point immediately after the hack as well as in subsequent quarterly and annual periods (hence our use of 'xxx' in naming the difference types, as we tested on both quarterly and annual timeframes).

As shown in tables 1A and 1B, there is no evidence for claiming that a hacked company incurs more costs in the quarterly or annual periods after the breach versus its own historic costs averaged over the preceding three years. A simplistic conclusion would be that companies are unaffected by hacks. However, comparing them to the set of companies that were not breached leads to different conclusions.

As the data show, the hacked company has a substantially higher cost base versus both its non-breached peers and the MSCI ACWI in the quarterly and annual periods following an attack. We see those results especially in the capex of a company, and to a lesser extent in the opex. In our view, these discrepancies between a company's costs relative to its own history and those versus peers are the result of elevated expenditure by the company related to resolving the hack. These costs are typically compensated for by savings made on other company projects.

In general, that implies that the overall cost level for a company stays elevated for a longer period of time following a cyber breach. Investors don't like volatile costs and margins, hence management teams smooth the costs over a number of quarters. The hacked companies show significantly higher capex and opex versus their non-hacked peers for an extended period of time, as shown by the data for the quarterly and annual periods directly after the hack.

We can therefore argue that hacked companies have significantly higher costs than companies which have not experienced a breach. In general terms, we show that capex levels for hacked companies are 11%-16% higher than for non-breached companies across benchmarks for subsequent quarterly and annual periods. The opex result is lower, at 8% -11%, and only significant in annual results.

Such conclusive results – despite our relatively small sample size and the potential for the peer group to be contaminated by hacks unknown to us – show how strong the cost implications are for hacked companies. Both factors, namely, reduce the statistical significance of our findings.

What we also see in the data is an interesting difference between capex and opex. For providers of software licences (one could extend this to a software-as-a-service (SAAS) environment, too), we would expect the direct costs of a hack to come at the expense of operational costs. However, even though our dataset starts in 2005, it is only since 2019 that we saw a significant uptake of cloud services and cybersecurity-focused SAAS offerings. Before 2019, most cybersecurity solutions were managed on premises.

Within the financial sector, a lot of companies' continue to manage on-premises solutions due to regulatory requirements. This explains why we see larger and more significant effects on capex as opposed to opex, especially in the quarterly data. We think that a replication of this study focusing of breaches after 2019 could, potentially, show a shift in expenditure from capex to opex.

In table 1B, we look at the impact of hacks on companies' sales and selling, general and administrative expenses (SG&A). As the data show, the results for both are significantly different relative to non-hacked peers.

This could come as a surprise, as we would expect a publicised breach to weaken sales. Similar results were obtained in private studies on the insurance sector (involving a mix of private and public companies). The main explanation for these findings is that SG&A increases after a hack to restore brand image.

A cyber-breach, when disclosed, corrodes a company's image yet also provides brand exposure. Marketing teams need to respond to the negative news by developing positive messages, often launching big campaigns to fortify their image. The sales impact, therefore, is not related to the hack but the increased SG&A spend.

One could look at this as an opportunity cost because it is possible that the company's sales numbers would have been better for a similar SG&A spend. Or less SG&A spend would have been required to achieve better sales numbers in case a breach did not happen.

The most important conclusion we can draw from table 1B is that these breaches have enduring effects. Not only in the quarter after the hack, but also in the year(s) afterwards we find evidence of elevated costs. In fact, this spending increases with time, as data for the next period show greater impacts in both size and significance.

3) Lasso regression results

After showing the effects on simple averages, we looked at whether it is possible to actually explain elevated capex, opex, sales and SG&A by factors other than the dummy variable which describes whether a company is hacked or not.

TABLE 1A: SIMPLE AVERAGES[6] FOR CAPEX AND OPEX IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Difference type	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP
_diff_qoq_overall			-0.949 *0.65*	3.449 *0.42*			-0.360 *0.86*	-1.624 *0.45*
_diff_qoq_sector			0.743 *0.76*	7.774 *0.14*			-0.835 *0.74*	-1.267 *0.72*
_diff_yoy_hist	0.684 *0.88*	1.621 *0.23*	-4.675 *0.37*	2.104 *0.39*	6.580 *0.12*	1.994 *0.37*	-9.355* *0.06*	1.582 *0.31*
_diff_yoy_hist_overall	13.093*** *0.01*	8.935*** *0.00*	11.248* *0.05*	1.739 *0.42*	15.693*** *0.00*	10.945*** *0.00*	3.246 *0.45*	2.870 *0.14*
_diff_yoy_hist_sector	12.603** *0.01*	9.723*** *0.00*	11.981** *0.03*	0.552 *0.81*	16.051*** *0.00*	11.769*** *0.00*	4.474 *0.28*	2.129 *0.29*
_diff_yoy_overall	12.563** *0.01*	8.481*** *0.00*	9.486* *0.09*	1.606 *0.52*	16.647*** *0.00*	11.156*** *0.00*	2.407 *0.57*	0.774 *0.73*
_diff_yoy_sector	11.427** *0.03*	10.572*** *0.00*	14.194** *0.01*	3.667 *0.14*	16.779*** *0.00*	11.614*** *0.00*	2.920 *0.54*	3.947 *0.13*

Source: LOIM, 2023.

TABLE 1B: SIMPLE AVERAGES FOR SALES AND SG&A IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	SALES	SGA	SALES	SGA	SALES	SGA	SALES	SGA
_diff_qoq_overall			1.288 *0.39*	2.240 *0.22*			7.901** *0.01*	3.400* *0.07*
_diff_qoq_sector			1.081 *0.57*	4.025*** *0.00*			7.959** *0.02*	4.646*** *0.01*
_diff_yoy_hist	-1.897** *0.02*	-1.187 *0.44*	-1.360 *0.40*	-1.817 *0.59*	-0.692 *0.57*	1.685 *0.45*	-0.952 *0.61*	1.562 *0.48*
_diff_yoy_hist_overall	5.207*** *0.00*	5.918*** *0.00*	8.218*** *0.00*	10.776*** *0.00*	6.456*** *0.00*	9.373*** *0.00*	10.105*** *0.00*	13.236*** *0.00*
_diff_yoy_hist_sector	5.461*** *0.00*	6.912*** *0.00*	8.790*** *0.00*	11.037*** *0.00*	6.397*** *0.00*	9.171*** *0.00*	10.823*** *0.00*	13.637*** *0.00*
_diff_yoy_overall	4.933*** *0.00*	5.806*** *0.00*	7.406*** *0.00*	9.831*** *0.00*	6.685*** *0.00*	9.574*** *0.00*	9.906*** *0.00*	13.775*** *0.00*
_diff_yoy_sector	5.121*** *0.00*	5.823** *0.02*	7.905*** *0.00*	11.909*** *0.00*	5.081** *0.02*	4.413 *0.23*	10.544*** *0.00*	15.781*** *0.00*

Source: LOIM, 2023.

[6] * 90% significance level | ** 95% significance level | *** 99% significance level

We use market capitalisation, and the time to the reported quarterly or annual results, sectors and sustainability measures by large providers aiming to differentiate companies on their cyber-readiness based on questionnaires, to explain differences in costs and the sales of breached companies.

Tables 2A and 2B show the results for the constant, which in this case reflects a hacked company, when all these other factors are added to the regression. As can be seen, the results are robust, supporting similar conclusions as those in the previous section.

TABLE 2A: LASSO REGRESSION FOR CAPEX AND OPEX IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Difference Type	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP
_diff_qoq_overall			-0.010 *0.63*	0.035 *0.25*			-0.004 *0.86*	-0.016 *0.38*
_diff_qoq_sector			0.007 *0.76*	0.078* *0.05*			-0.008 *0.72*	
_diff_yoy_hist	0.007 *0.86*			0.021 *0.37*	0.066* *0.10*	0.020 *0.36*	-0.094* *0.06*	0.016 *0.20*
_diff_yoy_hist_overall	0.131*** *0.01*	0.089*** *0.00*	0.113* *0.05*	0.017 *0.36*	0.157*** *0.00*	0.109*** *0.00*	0.033 *0.42*	0.029* *0.08*
_diff_yoy_hist_sector	0.126*** *0.01*	0.097*** *0.00*	0.120** *0.03*	0.006 *0.78*	0.161*** *0.00*	0.118*** *0.00*	0.045 *0.24*	0.021 *0.21*
_diff_yoy_overall	0.126*** *0.01*	0.085*** *0.00*	0.095* *0.09*	0.016 *0.41*	0.167*** *0.00*	0.144*** *0.00*	0.024 *0.54*	0.008 *0.69*
_diff_yoy_sector	0.114** *0.02*	0.106*** *0.00*	0.142** *0.01*		0.168*** *0.00*	0.116*** *0.00*	0.029 *0.51*	0.040* *0.10*

Source: LOIM 2023.

TABLE 2B: LASSO REGRESSION FOR SALES AND SG&A IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Difference type	SALES	SGA	SALES	SGA	SALES	SGA	SALES	SGA
_diff_qoq_overall				0.036** *0.03*			0.079** *0.01*	0.034** *0.03*
_diff_qoq_sector				0.040*** *0.00*			0.080** *0.02*	0.047*** *0.01*
_diff_yoy_hist	-0.019** *0.02*	-0.012 *0.40*	-0.014 *0.38*	-0.018 *0.56*	-0.007 *0.55*	0.017 *0.41*	-0.010 *0.59*	0.007 *0.73*
_diff_yoy_hist_overall	0.071*** *0.00*	0.059*** *0.00*	0.061*** *0.00*	0.108*** *0.00*	0.065*** *0.00*	0.130*** *0.00*	0.101*** *0.00*	0.132*** *0.00*
_diff_yoy_hist_sector	0.084*** *0.00*	0.092*** *0.00*	0.088*** *0.00*	0.110*** *0.00*	0.092*** *0.00*	0.092*** *0.00*	0.146*** *0.00*	0.136*** *0.00*
_diff_yoy_overall	0.073*** *0.00*	0.081*** *0.00*	0.074*** *0.00*	0.098*** *0.00*	0.097*** *0.00*	0.096*** *0.00*	0.133*** *0.00*	0.138*** *0.00*
_diff_yoy_sector	0.057*** *0.00*	0.095*** *0.00*	0.079*** *0.00*	0.119*** *0.00*	0.051** *0.01*	0.084** *0.05*	0.147*** *0.00*	0.158*** *0.00*

Source: LOIM 2023.

TABLE 3A: LASSO REGRESSION ON CAPEX AND OPEX VERSUS SECTOR PEERS IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**
const	0.114** *0.02*	0.106*** *0.00*	0.142** *0.01*		0.168*** *0.00*	0.116*** *0.00*	0.029 *0.51*	0.040* *0.10*
Distance to being made public	0.149*** *0.00*	0.032** *0.03*			0.130*** *0.01*		0.074* *0.10*	
Market cap in USD (freefloat)		-0.053*** *0.00*				-0.098*** *0.00*		
SUS_Data privacy & security policy								0.054** *0.03*
SUS_Data privacy programme					0.147*** *0.00*			
SUS_Cybersecurity programme								

Source: LOIM, 2023.

TABLE 3B: LASSO REGRESSION ON SALES AND SG&A VERSUS SECTOR PEERS IN THE EVENT OF A HACK

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	**SALES**	**SGA**	**SALES**	**SGA**	**SALES**	**SGA**	**SALES**	**SGA**
const	0.057*** *0.00*	0.095*** *0.00*	0.079*** *0.00*	0.119*** *0.00*	0.051** *0.01*	0.084** *0.05*	0.147*** *0.00*	0.158*** *0.00*
Distance to being made public		0.090*** *0.00*	0.066*** *0.00*				0.034 *0.17*	0.034 *0.13*
Market cap in USD (freefloat)	0.021* *0.09*	-0.060*** *0.00*			-0.086*** *0.00*			-0.042* *0.07*
Sector_Commercial & Professional Services								
Sector_Diversified Financials	-0.063*** *0.00*	-0.104** *0.02*				-0.182*** *0.01*	-0.126** *0.02*	
Sector_Health Care Equipment & Services	0.279*** *0.00*					0.360** *0.02*		
SUS_Data privacy & security policy	-0.030*** *0.00*							
SUS_Data privacy programme						0.097*** *0.00*		0.044* *0.09*
SUS_Cybersecurity programme	-0.026*** *0.00*		0.033* *0.08*					0.039 *0.12*

Source: LOIM, 2023.

Tables 3A and 3B show the Lasso regression results from the highlighted rows at the bottom of tables 2A and 2B in more detail. We exclude all non-significant values from the table to gain a clear view of the driving factors in this regression.

As is widely known, a Lasso regression penalises the addition of variables. Usually, the R2 of the regression increases if more variables are added because the explainability increases – even if marginally only – with the number of variables. The Lasso methodology does not allow for this: if factors are added which do not actively contribute to the ability to explain results beyond a certain threshold (the lambda), they are deleted.

In this case, what we see is that market capitalisation is an explanatory variable in the regression. This makes sense: bigger companies have operating leverage at their disposal, resulting in a

lower cost base relative to smaller firms. What we also see is that the longer the period between the hack and the quarterly or annual results, the greater the explanatory power of the model. In other words, the effects are more visible if enough time has elapsed for them to be understood by the time of the next report.

To include sustainability considerations, we add data privacy and cybersecurity factors to the regression. An important conclusion is that in most cases, companies scoring higher on data-privacy and cybersecurity programmes incur higher costs after a breach than hacked companies scoring lower on these factors.

This conclusion is especially strong when looking at the sales and SG&A variables. In the appendix, we show that these effects are stronger for companies in the software and services industry than those in the diversified financials industry. For two reasons, these findings are counter – intuitive:

1. We would expect companies that score highly for these sustainability factors to be targeted less, especially within their respective sectors. Hackers follow the path of least resistance: if hacking your peer is easier than hacking you, for a similar potential outcome, hackers prefer the easy target. (This does not apply to hacks by state actors, which are motivated by strategic rather than monetary reasons.)
2. Companies scoring highly on data-privacy and cybersecurity policies should be better prepared for a hack. They are supposed to have policies in place to quickly respond to an attack, preventing or mitigating the impact of a breach, and recovering faster. But we find the opposite is true, which is clear evidence of the mismatch between questionnaire-based and fact-based outcomes

Ask any company if they have data-privacy and cybersecurity policies in place, and they will say: "yes". Companies with large reporting departments tend to score better in questionnaire-based assessments, too. It is also interesting to see that high-scoring companies spend considerably more on SG&A when hacked versus low-scoring hacked companies, which supports the 'keeping up appearances' thesis – ie. restoring confidence in the brand is essential. Yet investors can see through the sheen by applying evidence-based techniques to assess the cybersecurity readiness of a company. We describe this in more detail in the next section.

We also researched whether the type of breach influenced the magnitude of the change in any of the cost variables. Our dataset differentiates between hack vectors (malware, skimmer, web and unknown), action (error, hacking, malware and misuse) and actor (external, internal, partner and unknown). However, none of these variables significantly explained the different cost impacts observed.

The most important factor, rather, is the absolute fact that a company has been hacked. This says a lot about the investment industry's progress in integrating hack data into stock fundamentals and pricing. At the moment, differentiation rests on whether a company has been hacked or not, but we know from practical and anecdotal evidence that the type of hack plays a substantial role in determining the total damage. In the case of a DDOS (distributed denial of service) attack, for example, the solutions are easier to fix than breaches using spy-, mal- or ransomware.

Currently, there is no mandatory disclosure requirement for companies to confirm the type of hack they have suffered, nor a detailed and audited assessment of the total damage. Regulators want to change this in the future: for instance, starting October 2024, the European Union will require member states to publish a coordinated vulnerability disclosure policy.[7] Since we have no access to such datasets yet, we need evidence-based approaches to gain a deeper understanding of the impacts of hacks on company fundamentals.

[7] European Union Agency for Cybersecurity, 16 February 2023. "Coordinated Vulnerability Disclosure: Towards a Common EU Approach".

The LOIM approach to integrating cybersecurity risk

As explained, we need measures to assess cybersecurity risk at the corporate level because they impact stock fundamentals. This approach must be evidence-based, because filling out questionnaires as part of the standard ESG approach has proven to be ineffective. We focus on evidence-based testing, as discussed in our previous white paper[1], and test known and exploited vulnerabilities for companies as a measure of basic cybersecurity hygiene.

Since we began using the methodology last year, we have made three meaningful observations:

1. Cybersecurity risks are like needles in a haystack
2. Companies who neglect cybersecurity risks for longer are more vulnerable
3. Engagement based on screening helps reduce vulnerabilities

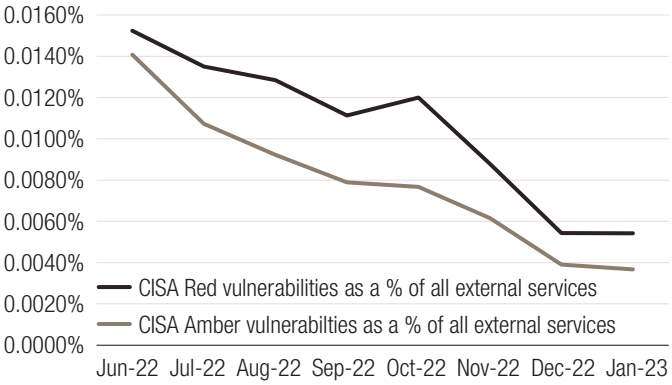
We provide details about each of these below.

1) Cybersecurity risks are like needles in a haystack

As shown in figure 4, the number of CISA vulnerabilities as a percentage of the total external services or touchpoints of a company is very low. We are talking about six known vulnerabilities in every 100,000 services, where a single company, on average, uses approximately 4000 services in our universe. Given the fact that we are assessing known and exploited vulnerabilities, it is critical for us that the company addresses vulnerabilities it is aware of.

FIG 4. CISA VULNERABILITIES MEASURED AGAINST TOTAL EXTERNAL SERVICES

TOTAL NUMBER OF CISA VULNERABILITIES EXPRESSED AS A % OF ALL EXTERNAL SERVICES IDENTIFIED WITHIN THE COHORT



Source: KYND as at 2023.

The unknown vulnerabilities, meanwhile, exist somewhere in that huge range of external services on the market, and companies would need to continuously screen every single one of them in order to prevent hacks. That amounts to a very costly and time-consuming task.

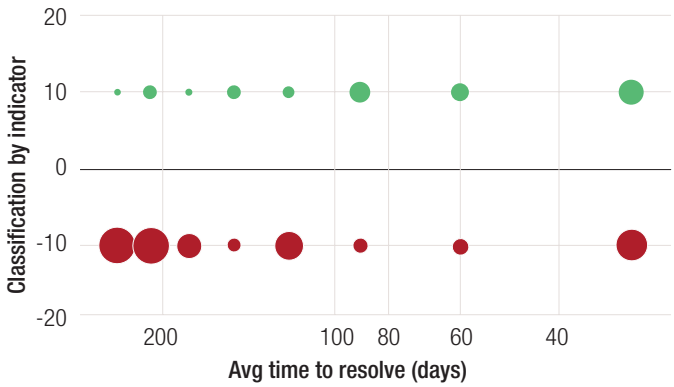
We are under no illusion that a company can be 100% protected from breaches, yet the benefits of trying to achieve this outweigh the costs, in our view. Protecting critical data is an absolute must-have and the lion's share of a firm's cybersecurity resources should go towards protecting those domains. In addition, the vulnerabilities identified by CISA are simply the low-hanging fruit: at a minimum, every company should scan its external services based on this list and ensure the vulnerabilities are patched. CISA hands six in 100,000 vulnerabilities to them on a gold platter, for free, so there really is no excuse to not making use of that information.

2) Companies which neglect cyber risks longer are more vulnerable

Figure 5 shows the difference in how companies respond to patching their cybersecurity vulnerabilities. It is a point-in-time representation of the screened universe, where 'green' companies, in general, do not show (structural) vulnerabilities, in contrast to 'red' companies. Green companies experiencing a vulnerability are clearly more responsive, as only a handful have left vulnerabilities unfixed for more than 80 days. Red companies, on the other hand, tend to allow vulnerabilities to continue for up to 200 days or longer, and can be considered less responsive to known and exploited weaknesses in their software.

FIG. 5 TIME TAKEN TO PATCH CYBERSECURITY VULNERABILITIES

DISTRIBUTION OF RED AND GREEN ORGANISATIONS AND THE AVERAGE TIME TO RESOLVE CISA RAGs



Source: KYND, 2023.

Another interesting takeaway is that a lot companies try to strengthen their software within 30 days of becoming aware of the risk. But those that don't are very likely to let that vulnerability persist for 100 days or longer.

Our methodology for managing cybersecurity risk involves engaging with companies on two occasions. First, when we identify a critical software issue in our screenings (an event indicated on the right side of figure 5). We email firms to describe the vulnerability and provide a guide on how to patch it. As investors, we find the beauty of an evidence-based approach to be the ability to monitor whether the companies took action instead of having to rely on their word through questionnaires. If our next monthly screen finds the same vulnerability, it is very likely that the company will have it for a longer period of time (as indicated on the left side of figure 5).

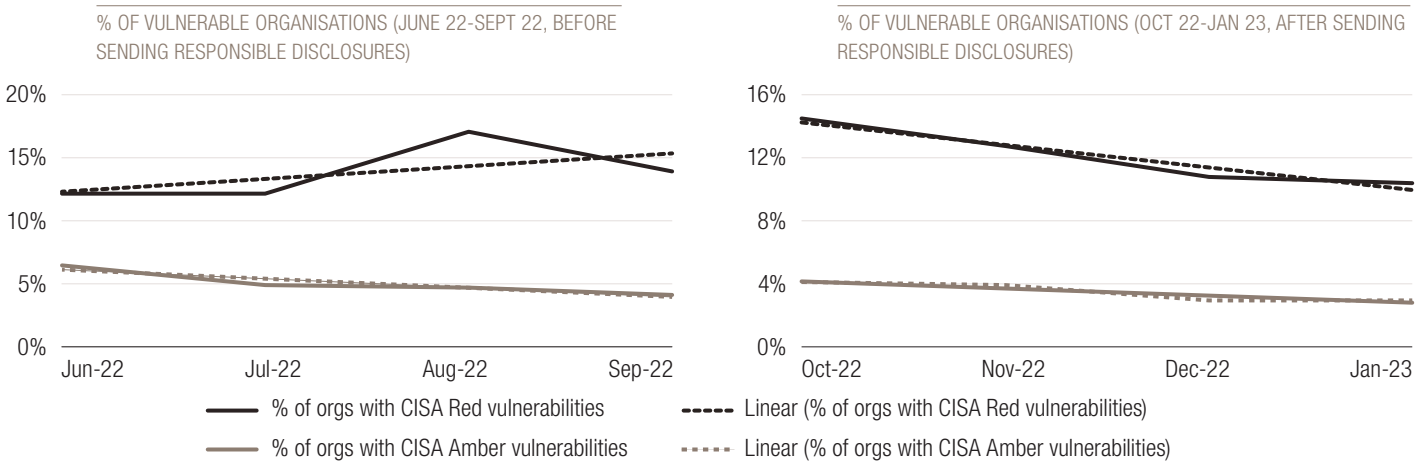
At that stage, we work with our stewardship team to start preparing an engagement to pressure the company to improve cybersecurity risk management by patching the vulnerabilities. Most companies are very responsive and in all our conversations so far, took it very seriously. Later screenings showed that the vulnerabilities were resolved.

In other cases, companies have not been responsive at all, indicating to us that they do not take cybersecurity seriously. In our view, this shows a weakness in corporate governance. Within the LOIM Global FinTech strategy, we reduce positioning in companies that do not respond positively to engagement and allow cybersecurity vulnerabilities to endure. We believe there is no excuse for not acting on free CISA information and encouragement from an engaged shareholder.

3) Engagement based on screening helps reduce vulnerabilities

Engagement works, as figure 6 shows. Since September last year, when we started to engage all red companies identified in our screens, the number of cybersecurity vulnerabilities has decreased. We recognise that this dataset is limited, and we are very aware of the fact that we need to keep a wide margin around conclusions based on a couple of observations, but the trend so far looks promising. As we continue to engage companies on this topic and other investors pay more attention to the matter, we expect the effect of engagement to strengthen over time.

FIG. 6 EFFECTS OF ENGAGEMENT ON CYBERSECURITY



Source: KYND as at 2023.

Conclusions

In this paper, our second on analysing cybersecurity risk and integrating it into fundamental stock analysis, we show the results of a statistical study on how hacks impact a set of listed FinTech companies. The results show that cybersecurity breaches have an insignificant effect on the share-price returns of the hacked companies, leading us to conclude that the market is neglecting cyber-breaches. This differs from the widely held view that hacks heavily influence stock prices, since major breaches have resulted in lawsuits from victims and regulators.

We then performed further tests to determine whether this market reaction was, in fact, correct by comparing the lack of stock-price movement to the hacked company's quarterly and annual reports. Here, we find that hacked companies disclose higher capex and opex as a direct result of having to restore the operational and brand damage caused by the attack versus non-breached peers who did not incur these costs.

Across benchmarks, we conclude that capex increases 11%-16% for hacked companies and opex rises 8% -11% relative to non-hacked peers. At the same time, we also find that companies try to mitigate the negative effects of a breach by significantly increasing their SG&A expenses in order to compensate for the bad publicity. That often leads, in the quarters after a hack (and in the annual results), to an uplift in sales.

This might seem positive outcome, but it must be noted that the same increase in sales could have been achieved with lower costs if a breach did not happen (especially less capex and opex). The effects of breaches on sales and SG&A become more evident over time, as subsequent quarterly and annual results show.

Crucially, the evidence from our study shows that there is a cost to being hacked, and that cost is not discounted properly in the market. Our view going forward is that these effects will become larger – especially in the opex line – as the transition to SAAS continues. Besides that, regulatory fines are likely to generate larger one-off costs, as well.

To manage these risks in portfolios, we believe asset managers should incorporate cybersecurity information into their investment processes. This won't prevent hacks, but it will help them distinguish well-prepared companies from vulnerable ones. From a valuation perspective, hacked companies should, all else being equal, trade at a discount versus their non-hacked peers, given the elevated costs arising from a breach.

We show in our research that questionnaire-based assessments of a company's cybersecurity preparedness can be misleading. We assess the scores on data privacy and protection, as well as the existence of cybersecurity programmes, as disclosed by companies in those questionnaires. We find evidence that high-scoring companies have a higher cost base than low-scoring, hacked companies. This is counter-intuitive for two reasons:

1. For a similar potential outcome, hackers focus on easier targets instead of tough ones (except for state actors, whose attacks are driven by strategic instead of monetary motives)
2. High-scoring companies should be better prepared to respond to, and recover from, a cyber breach. But the opposite is true, reinforcing our preference for evidence-based cybersecurity analysis over questionnaire results

Our analysis shows that it is very difficult for companies – let alone investors – to identify cybersecurity vulnerabilities. There are about six known exploited vulnerabilities in every 100,000 external services or touchpoints that a company deploys in our FinTech universe. That is a very small number of threats for a cybersecurity department to identify: it's like searching for six malign needles in a benign haystack.

In June 2022, around the time we published our first white paper on analysing cybersecurity risk, we began testing CISA vulnerabilities. These are known and exploited vulnerabilities which CISA provides at no charge. The fact that known and exploited vulnerabilities exist is disappointing, especially since we have established a significant link between breaches and increased costs. Therefore, we consider this measure of a company's basic cybersecurity hygiene to be crucial in our investment process.

Cybersecurity is one of many inputs into an investment decision. Financial characteristics, market trends, and many other factors play important roles in the decision to invest. However, given the impact of cyber risks on numerous other fundamental factors in an investment decision – especially the financial impacts on opex and capex – we believe it should be a key part of the conviction an active portfolio manager develops as they seek to optimise the risk-return puzzle for their investors.

Appendix

Appendix 1: metrics used to calculate results by difference type

To test the impact of hacks on a company's fundamentals, we applied the seven metrics below to each field of the companies' balance sheets.

$S_{C,T} \coloneqq A\ company\ C's\ data\ point\ at\ time\ T$

- $R_{C,T}^{(q|a)} = \frac{S_{C,T}}{S_{C,T-(1/4)}} \coloneqq (Quarterly|Annual)\ rate\ of\ change\ of\ company\ C$
- **_diff_yoy_hist**
  - A company **C**'s year-to-year change LESS the average of their year-to-year changes averaged over the 3 years prior to time **T**

$$\Delta_{C,T} = R_{C,T}^{a} - exp\left(\frac{1}{3}\sum_{t=T-1}^{T-4} \ln\left(R_{C,t}^{a}\right)\right)$$

- **_diff_yoy_hist_sector**
  - A company **C**'s A companies year-to-year change LESS all companies within the same GICS 2 sector summed year-to-year changes averaged over the 3 years prior to time **T**

$$\Delta_{C,T} = R_{C,T}^{a} - exp\left(\frac{1}{3}\sum_{t=T-1}^{T-4} \ln\left(\frac{\sum S_{c,t}}{\sum S_{c,t-4}}, \forall c \in same\ GICS2\ sector\right)\right)$$

- **_diff_yoy_hist_overall**
  - A company **C**'s year-to-year change LESS all companies in the whole MSCI universe summed year-to-year changes averaged over the 3 years prior to time **T**

$$\Delta_{C,T} = R_{C,T}^{a} - exp\left(\frac{1}{3}\sum_{t=T-1}^{T-4} \ln\left(\frac{\sum S_{c,t}}{\sum S_{c,t-4}}, \forall c \in whole\ MSCI\ universe\right)\right)$$

- **_diff_yoy_sector**
  - A company **C**'s year-to-year change LESS all companies within the same GICS 2 sector summed year-to-year change at time **T**

$$\Delta_{C,T} = R_{C,T}^{a} - \left[\frac{\sum S_{c,t}}{\sum S_{c,t-4}}, \forall c \in same\ GICS2\ sector\right]$$

- **_diff_yoy_overall**
  - A company **C**'s year-to-year change LESS all companies in the whole MSCI universe summed year-to-year change at time **T**

$$\Delta_{C,T} = R_{C,T}^{a} - \left[\frac{\sum S_{c,t}}{\sum S_{c,t-4}}, \forall c \in whole\ MSCI\ universe\right]$$

- **_diff_qoq_sector**
  - A company C's quarter-to-quarter change LESS all companies within the same GICS 2 sector summed quarter-to-quarter change at time T

$$\Delta_{C,T} = R_{C,T}^{q} - \left[\frac{\sum S_{c,t}}{\sum S_{c,t-1}}, \forall c \in same\ GICS2\ sector\right]$$

- **_diff_qoq_overall**
  - A company **C**'s quarter-to-quarter change LESS all companies in the whole MSCI universe summed quarter-to-quarter change at time **T**

$$\Delta_{C,T} = R_{C,T}^{q} - \left[\frac{\sum S_{c,t}}{\sum S_{c,t-1}}, \forall c \in whole\ MSCI\ universe\right]$$

Appendix 2: sector-specific Lasso regression results

We find the results on sustainability factors to contribute stronger in the IT sector versus diversified financials. The results below first show the optimal Lasso regressions within financials on capex, opex, sales and SG&A (appendix 2A and 2B), followed by a similar dataset on the software and services sector (appendix 2C and 2D).

APPENDIX 2A: LASSO REGRESSION RESULTS (SECTOR = DIVERSIFIED FINANCIALS; DIFFERENCE TYPE = _DIFF_YOY_SECTOR) - COSTS

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**	**CAPEX**	**OP_EXP**
const	0.119* *0.06*	0.107*** *0.00*	0.236* *0.05*		0.105* *0.07*	0.054** *0.01*	0.056 *0.50*	0.040* *0.10*
Distance to being made public	0.325*** *0.00*	0.070** *0.01*						
Market cap in USD (freefloat)	0.111* *0.09*	-0.082*** *0.01*				-0.051** *0.03*		
SUS_Data privacy & security policy		0.046* *0.10*				0.052** *0.02*	0.158* *0.07*	0.054** *0.03*

Source: LOIM, 2023.

APPENDIX 2B: LASSO REGRESSION RESULTS (SECTOR = DIVERSIFIED FINANCIALS; DIFFERENCE TYPE = _DIFF_YOY_SECTOR) - SALES/SGA

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	**SALES**	**SGA**	**SALES**	**SGA**	**SALES**	**SGA**	**SALES**	**SGA**
const	0.011 *0.24*	-0.003 *0.95*	0.041* *0.10*		-0.004 *0.80*	-0.108* *0.06*	0.025	
Distance to being made public		0.191*** *0.00*	0.128*** *0.00*		0.040** *0.03*		0.065** *0.02*	
SUS_Data privacy & security policy			0.055* *0.05*				0.070** *0.01*	
SUS_Data privacy programme	0.019* *0.06*		-0.080*** *0.00*				-0.061** *0.02*	

Source: LOIM, 2023.

APPENDIX 2C: LASSO REGRESSION RESULTS (SECTOR = SOFTWARE & SERVICES; DIFFERENCE TYPE = _DIFF_YOY_SECTOR) - COSTS

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP	CAPEX	OP_EXP
const	0.111 *0.13*	0.092*** *0.00*			0.157** *0.02*	0.109*** *0.00*	0.044 *0.43*	
Distance to being made public					0.120* *0.08*			
Percentrank in all GICS sector level 2					-0.165** *0.02*		0.117** *0.04*	
SUS_Data privacy & security policy	-0.130* *0.09*	-0.039** *0.04*						
SUS_Data privacy programme					0.240*** *0.00*			

Source: LOIM, 2023.

APPENDIX 2D: LASSO REGRESSION RESULTS (SECTOR = SOFTWARE & SERVICES; DIFFERENCE TYPE = _DIFF_YOY_SECTOR) - SALES/SGA

	First following period				Next following period			
	ANNUAL		QUARTERLY		ANNUAL		QUARTERLY	
Coefficient	SALES	SGA	SALES	SGA	SALES	SGA	SALES	SGA
const	0.050*** *0.00*	0.073*** *0.00*	0.079*** *0.00*	0.091** *0.01*	0.036* *0.08*	0.099** *0.01*	0.134*** *0.00*	0.133*** *0.00*
Distance to being made public			-0.035* *0.09*		0.041* *0.05*			
MAT_PERCENTRANK_GICS2						-0.075* *0.06*		
Market cap in USD (freefloat)	0.022* *0.07*		0.028 *0.19*					
SUS_Data privacy & security policy	-0.041*** *0.00*		-0.048** *0.03*					
SUS_Data privacy programme			0.024 *0.31*			0.143*** *0.00*		0.049* *0.06*
SUS_Cybersecurity programme	-0.021* 0.07		0.044* *0.06*					0.048* *0.07*

Source: LOIM, 2023.

IMPORTANT INFORMATION

For professional investor use only.

This document is issued by Lombard Odier Asset Management (Europe) Limited, authorised and regulated by the Financial Conduct Authority (the "FCA"), and entered on the FCA register with registration number 515393.

Lombard Odier Investment Managers ("LOIM") is a trade name. This document is provided for information purposes only and does not constitute an offer or a recommendation to purchase or sell any security or service. It is not intended for distribution, publication, or use in any jurisdiction where such distribution, publication, or use would be unlawful. This material does not contain personalized recommendations or advice and is not intended to substitute any professional advice on investment in financial products. Before entering into any transaction, an investor should consider carefully the suitability of a transaction to his/her particular circumstances and, where necessary, obtain independent professional advice in respect of risks, as well as any legal, regulatory, credit, tax, and accounting consequences. This document is the property of LOIM and is addressed to its recipient exclusively for their personal use. It may not be reproduced (in whole or in part), transmitted, modified, or used for any other purpose without the prior written permission of LOIM. This material contains the opinions of LOIM, as at the date of issue. Neither this document nor any copy thereof may be sent, taken into, or distributed in the United States of America, any of its territories or possessions or areas subject to its jurisdiction, or to or for the benefit of a United States Person. For this purpose, the term "United States Person" shall mean any citizen, national or resident of the United States of America, partnership organized or existing in any state, territory or possession of the United States of America, a corporation organized under the laws of the United States or of any state, territory or possession thereof, or any estate or trust that is subject to United States Federal income tax regardless of the source of its income. Source of the figures: Unless otherwise stated, figures are prepared by LOIM. Although certain information has been obtained from public sources believed to be reliable, without independent verification, we cannot guarantee its accuracy or the completeness of all information available from public sources. Views and opinions expressed are for informational purposes only and do not constitute a recommendation by LOIM to buy, sell or hold any security. Views and opinions are current as of the date of this presentation and may be subject to change. They should not be construed as investment advice. No part of this material may be (i) copied, photocopied or duplicated in any form, by any means, or (ii) distributed to any person that is not an employee, officer, director, or authorised agent of the recipient, without Lombard Odier Asset Management (Europe) Limited prior consent. In the United Kingdom, this material is a marketing material and has been approved by Lombard Odier Asset Management (Europe) Limited which is authorized and regulated by the FCA.