MORNINGSTAR | SUSTAINALYTICS

METHODOLOGY

The Impact of Cyberattacks on Stock Prices

October 2022

Liam Zerter, CFA
Quantitative Research Manager,
Methodology & Product Architecture

Melissa Hudson, CISSP, CIPP/E
Associate Director,
Sector Research

About Morningstar Sustainalytics

Morningstar Sustainalytics is a leading ESG research, ratings, and data firm that supports investors around the world with the development and implementation of responsible investment strategies. For 30 years, the firm has been at the forefront of developing high-quality, innovative solutions to meet the evolving needs of global investors. Today, Morningstar Sustainalytics works with hundreds of the world's leading asset managers and pension funds who incorporate ESG and corporate governance information and assessments into their investment processes. The firm also works with hundreds of companies and their financial intermediaries to help them consider sustainability in policies, practices, and capital projects. With 17 offices globally, Morningstar Sustainalytics has more than 1,800 staff members, including more than 800 research analysts with varied multidisciplinary expertise across more than 40 industry groups. For more information, visit www.sustainalytics.com.

The information, methodologies, data and opinions contained or reflected herein are proprietary of Sustainalytics and/or its third party intended for non-commercial use, and may be made available to third parties only in the form and format disclosed by Sustainalytics. They are provided for informational purposes only and (1) do not constitute investment advice; (2) cannot be interpreted as an offer or indication to buy or sell securities, to select a project or make any kind of business transactions; (3) do not represent an assessment of the issuer's economic performance, financial obligations nor of its creditworthiness (4) are not a substitute for a professional advise; (5) past performance is no guarantee of future results.

These are based on information made available by the issuer and/ or by third parties, subject to continuous change and therefore are not warranted as to their merchantability, completeness, accuracy, up to dateness or fitness for a particular purpose. The information and data are provided "as is" and reflect Sustainalytics` opinion at the date of their elaboration and publication. Sustainalytics nor any of its third-party suppliers accept any liability for damage arising from the use of the information, data or opinions contained herein, in any manner whatsoever, except where explicitly required by law. Any reference to third party names is for appropriate acknowledgement of their ownership and does not constitute a sponsorship or endorsement by such owner. A list of our third-party data providers and their respective terms of use is available on our website. For more information, visit http://www.sustainalytics.com/legal-disclaimers.

Sustainalytics may receive compensation for its ratings, opinions and other deliverables, from, among others, issuers, insurers, guarantors and/or underwriters of debt securities, or investors, via different business units. Sustainalytics has put in place adequate measure to safeguard the objectivity and independence of its opinions. For more information visit Governance Documents or contact compliance@sustainalytics.com.

Sustainalytics
info@sustainalytics.com
www.sustainalytics.com

Stockholm
Copenhagen
Amsterdam
Zielona Gora
London
Toronto
Frankfurt
Boston
Brussels
Bucharest
Paris
Washington
New York
Timisoara
Tokyo
Mumbai
Sydney

The Impact of Cyberattacks on Stock Prices

Strong Data Privacy & Security Management Pays off

Authors:[1]

Liam Zerter, CFA
Quantitative Research Manager,
Methodology & Product Architecture
Liam.Zerter@morningstar.com

Melissa Hudson, CISSP, CIPP/E
Associate Director, Sector Research
Melissa.Hudson@morningstar.com

Data privacy and cybersecurity-related issues have become major drivers of business risk in recent years. Based on Morningstar Sustainalytics' Data Privacy and Security (DP&S) incident data, this report reviews recent DP&S incident trends and assesses the impact of significant cyberattack Incidents[2] on stock returns over time.

Our analysis reveals that strong Data Privacy and Security Management Indicator Scores are a favorable signal, positively correlated to one-year post-incident returns and significant risk reduction.

Highlights

- Since 2013, there has been a significant **increase** in the **severity** and **frequency** of **cyber-Incidents** with increasing acceleration into higher risk levels starting in 2018 for a risk rank of six or higher—on a scale of 'one' (low) to 'ten' (high) for business risk impact.
- The yearly **share** of total **Data Privacy and Security (DP&S) Incidents amongst all incidents** has **grown from 1.6% in 2013 to 3.5% in 2021**: A Cumulative Aggregate Growth Rate (CAGR) of 37%.
- We examine the average stock reaction over 120 trading days based on a time-series analysis of news releases of **69 high-risk cyberattacks**.
- We find an initial decline of -2.3% by day four post incident date, bottoming on the 60th trading day close, down -4.6%.
- The returns for the 'incident portfolio' the year after the cyberattack events was -0.65%, whereas the average return of those stocks in the prior year leading up to the incident date was 8.47%, signalling a significant and persisting impact from high-risk cyberattacks.
- Our research reveals that **stronger ESG Management Indicator Scores in Data Privacy and Security (DP&S) Policy are beneficial signals and positively correlate to one-year returns** post cyberattack incident.
- Stronger ESG Management Indicator Scores in DP&S have **risk benefits** in high-risk cyberattacks Incidents via **lower standard deviations** and **shallower average Max Drawdown.**

Introduction

Cyber risk as a material ESG risk

Cybersecurity risk is one of the most immediate and financially material environmental, social and governance (ESG) risks that organizations face today, an assessment shared by the World Economic Forum (WEF).[3]

Based on Morningstar Sustainalytics and market data, this report: (a) highlights the increasing number of Incidents connected to Data Privacy and Security (DP&S); (b) reviews the impact on the average share price reaction for a group of companies after news breaks of a potentially significant data breach or cyberattack; (c) examines the relationship between DP&S risk on future returns and share price volatility.

Companies with higher Data Privacy and Security scores perform better

Our analysis shows that companies with higher DP&S scores perform better. In turn, the results suggest better risk mitigation for corporations simply by investing in robust DP&S programs, along with a meaningful insight to investors, in that they should be attuned to the DP&S Indicator Management Scores of the companies in their portfolios, particularly when a cyberattack on a holding company has become public news.

News Incidents Analysis

Morningstar Sustainalytics' Controversies Research

Our analysts track daily global news feeds, spotting controversial material identifying companies involved in incidents that may negatively impact stakeholders, the environment, or the company's operations. These incidents feed Morningstar Sustainalytics' **Controversies Research,** which identifies companies involved in incidents that may negatively impact stakeholders, the environment or the company's operations and penalize company ratings within our **ESG Risk Rating** product. This news incidents analysis is sorted into 51 main thematic tags and ranked from one (lowest) to ten (highest) on their potential financial risk.

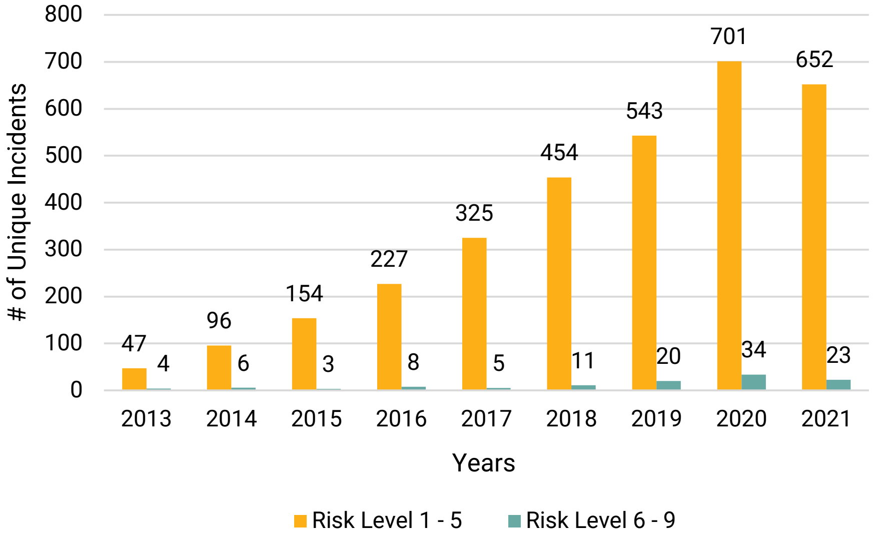
Data Privacy and Security ranks second in growth of the sizeable thematic controversy tags

Based on Morningstar Sustainalytics news incident analysis, we find that of the sizeable thematic controversy tags, DP&S ranks second in growth. Data Privacy and Security's yearly share of total incidents has increased from 1.6% in 2013 to 3.5% in 2021, a Cumulative Aggregate Growth Rate (CAGR) of 37%, placing it fourth in proportional incident growth across 51 themes.

DP&S's growth rate is well above the total incident growth curve CAGR of 24%.[4] Notably, while some incidents tags are empirically more likely to occur within specific industries, DP&S issues affect a growing spectrum of industries. Cybersecurity issues have become increasingly common due to rising digitization, which is also expanding to the supply chain and within other industries (e.g., integration, operational technology, and the internet of things enablement).

Exhibit 2 illustrates the distribution of DP&S Incidents, grouped by relative **Risk Level,** which represents a business risk to the company due to the Incidents (see the ESG Risk Rating Methodology),[5] with higher scores, representing higher levels of business risk to a particular company.

Exhibit 2: Incidents per Year – 2013 to 2021 – A Tale of Two Eras



Source: Morningstar Sustainalytics

From 2019 to 2021, the average yearly number of cybersecurity Incidents has increased significantly

We see a tale of two eras: Pre-and post-2018. From 2013 to 2017, higher risk Incidents (those ranked six or higher) averaged approximately five per year. From 2019 to 2021, the average yearly number of Incidents is closer to 26. Meanwhile, low-level Incidents continued growing, and medium-level Incidents became increasingly common.

While technology adoption explains more targets for attackers, many other drivers exist, propelling increased risk, damage, and complexity. These changes, in turn, create a new landscape in which cyberattack risk has suddenly become a risk that significantly evolved in the last five years.

Price Reaction to News of a Major Cyberattack

Analyzing the impact of cyberattack news on a company's stock price

This section focusses on the market's reaction to major cybersecurity Incidents. Based on a time-series analysis of share price response in our high-risk 'incident portfolio', we analyze the stock price trajectory against standard benchmarks and its volatility over time. This analysis measures: (i) the immediate price shock of a DP&S incident around cyberattacks and privacy breaches as a theme; (ii) the influence on likely returns; and (iii) a timeframe for how long a company experiences negative sentiment by investors.

A cross-sectional time series analysis to quantify the impact of a high-risk cyberattack

Stock price reaction to a material event can be an interpretation of how the market reacts to this new information. Moreover, it may be viewed as a meaningful signal about the financial materiality of a particular issue, as the market is effectively trying to quantify the financial cost of the event. By conducting a cross-sectional time series analysis, we aim to quantify the average impact of news regarding a high-risk cyberattack.

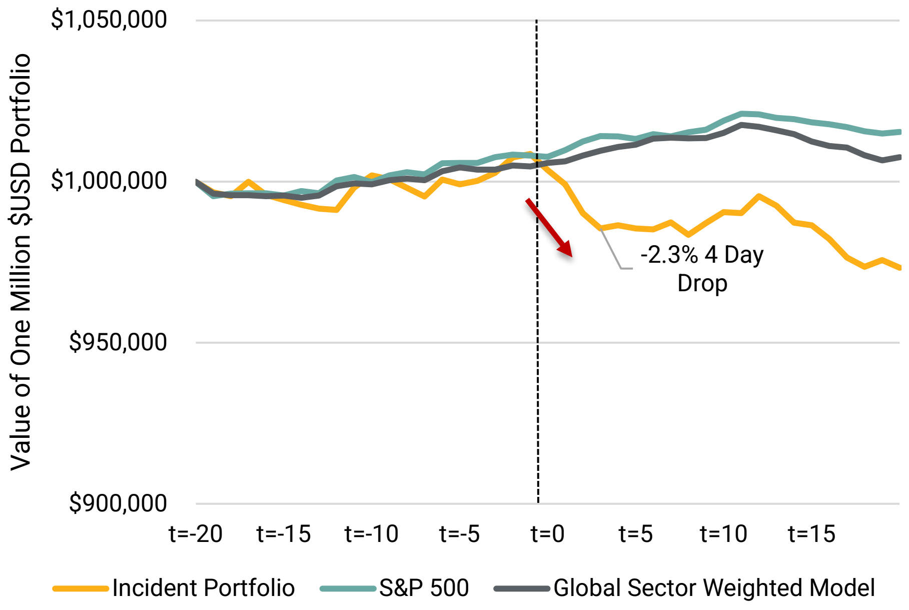
Using cyber and data breach-related incident reports that were assigned a risk score of 5 or more out of a possible 10, we gathered 69 occurrences of publicly traded companies with 100 trading days available post news release. We then built a time series of this 'incident portfolio' as illustrated in Exhibits 3 and 4 below, analyzing: (1) the short and (2) mid-term average share price reactions.

We align the 69 highest risk Incidents at t=0 and invest equally in these companies at t=-20, or 20 trading days before the incident becomes public, to ensure we capture any information leakage.

Each position is sector- and market-matched for weightings and timing

Then, to analyze the total loss against the market and each company's respective sector peers, we align the stock market index tracking the performance of 500 large companies listed in the United States (S&P 500) and the respective global sector benchmark for each company across exact dates, creating three time-matched portfolios, equally weighting each specific incident.

Exhibit 3: Time Series (Short-Term) - Share Price Reaction to Cyberattacks



*Companies are selected based on clear evidence describing a cyberattack
**Duplicate companies were permitted, given that each cyberattack is unique for that company

Source: Morningstar Sustainalytics

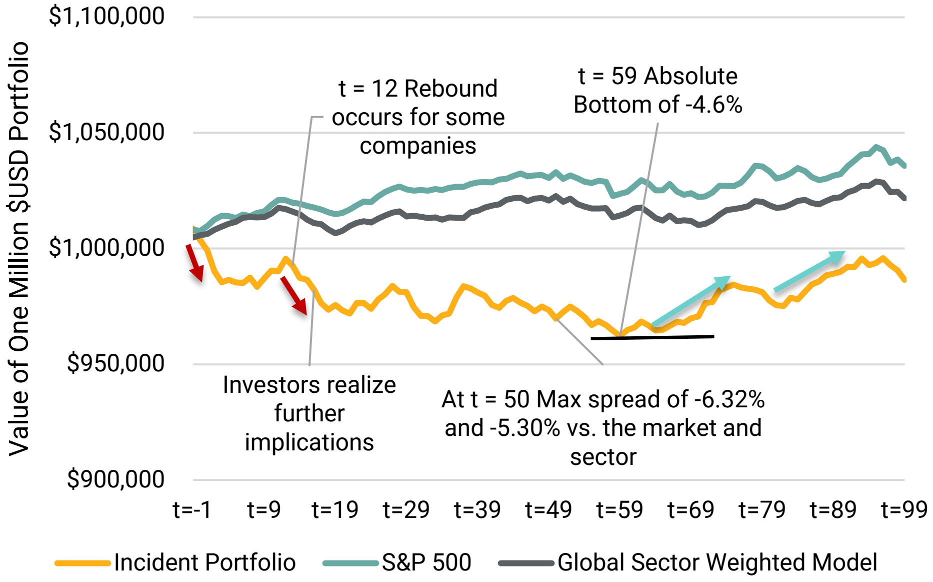
A drop of -2.3% in the first 4 days

Exhibit 3 above highlights the average stock price movement in the short term. The initial drop for the first four days is -2.3% in absolute terms. Looking at abnormal returns, the Cumulative Abnormal Return (CAR) of a high-risk 'incident portfolio' is -2.6% (see Exhibit 5 for more details).

A notable volatility spike in the twenty trading days after the Incident date

We find an apparent uptick in volatility, as the annualized standard deviation increased from 27.95 in the twenty days prior to the incident, to 34.28 in the twenty trading days after the Incident date (see Appendix, Exhibit 9). Further, we also see the average Max Drawdown scale from -7.57% to -9.84% for the same short-term periods (see Appendix, Exhibit 10).

Exhibit 4: Time Series (Medium-Term) - Share Price Reaction to Cyberattacks



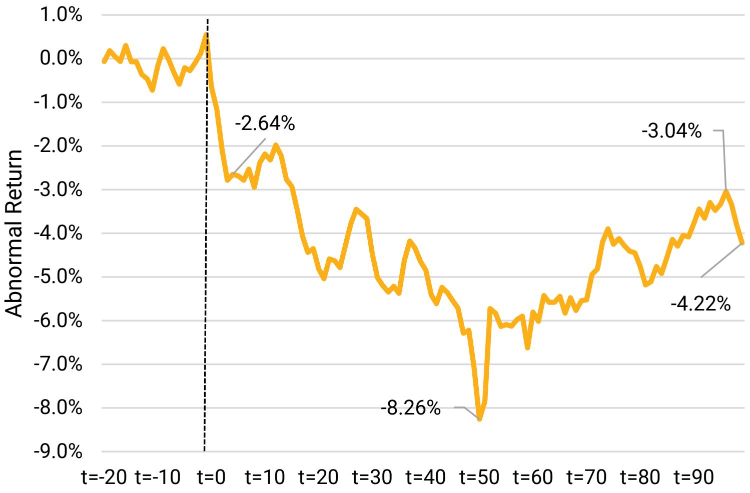
*Companies are selected based on clear evidence describing a cyberattack
**Duplicate companies permitted, given that each cyberattack is unique

Source: Morningstar Sustainalytics

Trading day 51 is the largest gap in returns against the benchmarks/market

On the 51st trading day, we see the most significant spread differential between the 'incident portfolio' and the S&P 500 and benchmark sector portfolios at -6.32% and -5.3%, respectively, with the absolute bottom on trading day 59.

Exhibit 5: Cumulative Abnormal Return – Equal Weighted



*Alpha and Beta calculations are calculated against S&P 500 daily returns for 180 trading days before the Incident.[6]

Source: Morningstar Sustainalytics

By conducting a CAR in Exhibit 5 to highlight risk-adjusted performance with respect to market movements, we find no meaningful abnormal returns for the first twenty days prior to the incident, followed by significant abnormal returns on the day of the incident. We also find that the 51st trading day is the absolute bottom with a CAR of -8.2%. Again, a reversal pattern occurs, stretching from trading day 51 to trading day 97.

Downward pressure abates after t=50

The 51st trading day marks the beginning of an ideal entry point. From this point forward—across the next 49 trading days to trading day 100—the average company return is 4.9%, and abnormal returns are 4.04%, with 54% of companies experiencing an increase in share price, with effectively half of the companies having positive abnormal returns.

A rebound begins for some companies

Comparing the average company-level correlation in the 50-day average trailing price change, we see an interesting distribution of correlations as follows:

- In the first 50 days post-incident, more company's correlations cluster closer to zero or negative, with a mean correlation of 22%, signalling a disconnect from the market.
- For days 50 to 100, we see an average correlation of 40%. This may signal stock prices returning to more normal correlation patterns to the market.

At first, it appears that around day 50, the downward pressure has lifted. Yet, from trading days 50 to 100, only half of the companies registered positive abnormal returns, signalling an isolated rebound experienced by a smaller subset of companies.

A Persistent Performance Gap

Looking beyond 100 days

Exhibit 6 shows that returns for the 'incident portfolio' one year following the cyberattack returned -0.65%, a considerable difference of 8.47% compared to the prior year, which returned 7.82%. Although the return in the prior year lags the sector benchmark by -3.9%, this is still within reasonable levels given the small sample size. Yet, the gap widened significantly in the post-incident period, highlighting the persisting impact of the cyberattacks.

One year later, the difference in the benchmarks is sizeable

Exhibit 6: Longer-Term Returns Analysis

	Annualized Returns	
	1 Year Before Incident	1 Year After Incident
Incident Portfolio (a)	7.82	-0.65
S&P 500 (b)	14.44	11.58
Sector Benchmark Portfolio (c)	11.73	10.15
Difference to S&P 500 = (a) - (b)	**-6.62**	**-12.23**
Difference to Sector = (a) - (c)	**-3.90**	**-10.80**

*Currency in use: Base Currency[7]

Source: Morningstar Sustainalytics

In the 100-day analysis, we see evidence of the negative downside fading and a return to trading in line with the market; however, one year later, we see that the ‘incident portfolio’ still lacks participation in upward moves by the market and peers.

This indicates that a dragging force impaired the ‘incident portfolio’ companies’ performance *beyond* the 100 trading days that we examined for stock price reaction. Therefore, a short-term trade may exist for high-risk cyberattacks around the three-month mark. Yet, investors should still be cautious for longer-term investments, as less than one-third of companies could keep pace with their respective sector benchmarks.

Data Privacy and Security Preparedness Pays off

Companies with higher Data Privacy and Security scores kept pace to their sector benchmark one year later

Looking into the long-term impacts in our ‘incident portfolio’, we find a statistically significant positive correlation between Morningstar Sustainalytics DP&S Management Indicator Scores and returns. Companies that implemented thoughtful data protection initiatives were better prepared to withstand cyberattacks. On average, companies with a better management score kept pace to their sector benchmark one year later. Conversely, those with adequate and lower scores significantly underperformed. This suggests a significant payoff for creating well-developed DP&S programs.

A clear positive correlation between returns and the DP&S management score

There is a positive correlation between company DP&S Management Indicator Scores prior to the cyber incident and the one-year returns post-incident. By using the Data Privacy and Security Policy Management Indicator Scores for the 69 companies as a signal for cybersecurity strength, our results show a positive correlation of 33% and that the Pearson correlation is statistically significant and different from 0 (see Appendix, Exhibit 11).

In Exhibit 7, we split the companies into three groups to test whether the DP&S management indicator provides more information about the relationship between the strength of a company's cybersecurity program and its effect on the stock price following a cyberattack.

Companies with strong Management Indicator Scores kept closer pace with their sector

Exhibit 7: DP&S Policy Management Indicator Scores – 1-Year Returns

	Data Privacy & Security Policy Management Score Split					
	Annualized Returns		Sector Benchmark		Difference	
	1 Year Before Incident	1 Year After Incident	1 Year Before Incident	1 Year After Incident	1 Year Before Incident	1 Year After Incident
Score 75 to 100	29.55	11.56	14.69	13.31	**14.87**	**-1.74**
Score of 25 to 50	-0.19	8.32	13.66	16.05	**-13.84**	**-7.73**
Score of 0 or N/A	4.04	-4.89	9.50	7.53	**-5.46**	**-12.42**

* Management Indicator Scores include predicted, retroactively researched, and actual historical scores before the incident date[8]
**N/A is representative of companies where no predicted or historical research for the Management Indicator Score was available
***Currency in use: Base Currency[9]

Source: Morningstar Sustainalytics

Better post-incident returns for companies that implemented cybersecurity programs

Of the twelve companies with scores of 75 to 100—strong to very strong implemented cybersecurity program—we find IT firms, such as Oracle and

Microsoft with resilient cybersecurity programs. However, we also find non-tech companies such as Orange SA, and Equifax. This small group of companies performed almost in line with their sector benchmark one-year post-incident, while those with lower scores significantly underperformed their sector peers.

Companies with strong Management Indicator Scores show lower volatility levels after a cyberattack Incident

We also find that companies with stronger Management Indicator Scores generally show lower volatility levels post-incident—as measured by standard deviation—with a correlation of -28% (Appendix, Exhibit 12) and lower Max Drawdown with a correlation of 27% (Appendix, Exhibit 13) when looking at the study group. On average, adverse stock price reactions to the downside were minimized.

Exhibit 8 showcases these risk measures across higher to lower Management Indicator Scores. For example, we see that companies with a DP&S Management Indicator Scores of 75 to 100—compared to those with scores of 0 or N/A—have a 35% lower average standard deviation. On average, the better scoring group also experienced an average max decline that was 62% shallower than those companies scoring 0 or N/A.

Exhibit 8: DP&S Policy Management Indicator Scores – 1 Year Risk Measures

	Post Incident Risk Measures	
	Standard Deviation	Average Max Drawdown
Score 75 to 100	7.09	-22.38
Score of 25 to 50	9.31	-29.53
Score of 0 or N/A	10.91	-32.88

* Management Indicator Scores include predicted, retroactively researched, and actual historical scores before the incident date[10]
**N/A is representative of companies where no predicted or historical research for the management score was available
***Currency in use: Base Currency[11]
**** Standard Deviation return calculations are made monthly[12]

Source: Morningstar Sustainalytics

Limiting the damage of a cyberattack and maintaining stakeholders' trust

It appears that in an environment where cyber risk and complexity have quickly escalated, those companies further along in their development of robust cybersecurity-related programs were better prepared to limit the damage of the cyberattack and maintain stakeholders' trust.

Conclusion

Growing cyber-Incidents call for enhancing preparedness

Cyberattack risk is one of the most immediate and financially material ESG risks. The growing frequency and severity of cyber-Incidents call for implementing and enhancing preparedness among companies.

A major cyberattack influences a stock price to the downside for 50 trading days

Based on Morningstar Sustainalytics and market data, we analyzed the changing dynamics of cyberattacks and the rising trend in the frequency and severity of Incidents. Then, we looked at the stock price effect of significant cyber-Incidents.

On average, a major cyberattack influences a stock price to the downside for about 50 trading days; then there is evidence of a bottom and a rebound. However, one year later, the ‘incident portfolio’ group significantly lags behind the market and sector benchmarks.

Strong Data Privacy and Security scores positively correlated to one-year returns post-Incident

Next, we show that Data Privacy and Security (DP&S) preparedness pays off. On average, strong DP&S management performance scores are a clear signal, positively correlated to one-year returns post-Incident. Moreover, we find that, on average, companies with higher DP&S Management Indicator Scores perform better in relation to the sector benchmark one year later. Conversely, those with adequate and lower scores significantly underperform. This suggests a significant payoff in mitigating risks by creating well-developed DP&S programs.

Appendix

Additional Charts & Figures

Exhibit 9: f-Test of Twenty Trading Days Standard Deviation (Daily Returns) Before and After Incident

F-Test Two-Sample for Variances

	t=-20	*t=20*
Mean	1.81	2.19
Variance	0.77	3.18
p<.001		

*The following standard deviations are calculated initially using daily returns but are converted in the text to annualized numbers

Source: Morningstar Sustainalytics

Exhibit 10: f-Test of Twenty Trading Days Max Drawdown Before and After Incident

F-Test Two-Sample for Variances

	t=-20	*t=20*
Mean	-7.57	-9.97
Variance	29.62	112.46
p<.001		

Source: Morningstar Sustainalytics

Exhibit 11: t-Test between Data Privacy and Security Management Score and One Year Returns

t-Test: Paired Two Sample for Means

	Returns After Incident	*Management Score*
Mean	- 0.65	24.26
Pearson Correlation	0.33	
t Stat	- 5.38	
p<.001 two-tail		

Source: Morningstar Sustainalytics

Exhibit 12: t-Test between Data Privacy and Security Management Score and Standard Deviation

t-Test: Paired Two Sample for Means

	Standard Deviation	*Management Score*
Mean	9.80	24.26
Pearson Correlation	- 0.28	
t Stat	- 3.36	
p<.001 two-tail		

*Return calculations are made monthly

Source: Morningstar Sustainalytics

Exhibit 13: t-Test between Data Privacy and Security Management Score and Max Drawdowns

t-Test: Paired Two Sample for Means

	Max Drawdown	*Management Score*
Mean	- 30.44	24.26
Pearson Correlation	0.27	
t Stat	- 13.46	
p<.001 two-tail		

*Max Drawdown is for 1-year post-incident

Source: Morningstar Sustainalytics

Glossary of Terms

Cumulative Abnormal Return (CAR)

Cumulative Abnormal Return (CAR) is the total of all abnormal returns. An abnormal return describes the unusually large profits or losses generated by a given investment or portfolio over a specified period. The performance diverges from the investments' expected, or anticipated, rate of return less the estimated risk-adjusted return based on an asset pricing model.

Cumulative Aggregate Growth Rate (CAGR)

The compound annual growth rate (CAGR) is the rate of return (RoR) that would be required for an investment to grow from its beginning balance to its ending balance, assuming the profits were reinvested at the end of each period of the investment's life span.[13]

Controversies Research

Mornignstar Sustainalytics Controversies Research identifies companies involved in incidents that may negatively impact stakeholders, the environment or the company's operations.

ESG Risk Rating

Mornignstar Sustainalytics' rating framework that measures the extent to which enterprise value is at risk, driven by environmental, social and governance (ESG) factors. The rating takes a two-dimensional approach. The exposure dimension measures a company's exposure to ESG risks, while the management dimension assesses a company's handling of these ESG risks.

Data Privacy and Security Policy (DP&S)

This indicator assesses a company's public position on the collection, use, disclosure and safeguarding of a consumer's personal information. It also assesses the extent to which a consumer is made aware of their privacy rights and how to exercise them. Personally Identifiable Information (PII) is information that identifies, links, relates to, is unique to, or describes a person.

A company's public-facing statement is a strong signal of their commitment to privacy and cybersecurity. In many cases, such a statement is a legal or regulatory requirement. In other cases, it is a long-standing best-practice. It shows that the company is willing to make a public commitment to privacy and cybersecurity and recognizes the harm that may occur if privacy rights are violated, including financial, legal, and reputational.

Incident

Reflects a company's involvement in cases of specific alleged misconduct with negative environmental and/or social impacts. Incidents form the most granular level of analysis we conduct. They are identified based on a comprehensive daily media analysis. Our analysts provide two assessments at the incident level, a stakeholder impact assessment and a reputational risk assessment. Incidents typically inform the Event Indicator outcome for a period of three years.

Management Indicator Score

An indicator that provides a signal about a company's management of an ESG issue through policies, programmes or quantitative performance. Management indicator raw scores range from 0 to 100, with 0 indicating no (evidence of) management of the issue and 100 indicating very strong management.

Max Drawdown

The peak to trough decline during a specific record period of an investment or fund. It is usually quoted as the percentage between the peak to the trough.

Risk Level (Incidents)

Business risk to the company as a result of the incidents.

Endnotes

[1] The authors would like to thank the following people for their comments on earlier drafts of this report: Aymen Karoui, Michelle McCulloch, Hendrik Garz, and Cristina Zabalaga.

[2] Text that is highlighted in bold teal indicates a term that is explained in the Glossary of terms in the Appendix.

[3] World Economic Forum (2022); Global Cybersecurity Outlook: Insight Report 2022; accessed (13.07.2022) at: https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

[4] Note that the growth rate of 24% is mainly influenced by Sustainalytics growing company coverage.

[5] See Garz H., Volk C.; (December 2020), "ESG Risk Ratings Methodology, Version 2.1", Morningstar Sustainalytics; accessed at: https://globalaccess.sustainalytics.com/#/research/risk

[6] Due to temporary halting of one stock and highly limited volatility for another, betas for two of the companies in question were substituted within the CAR model with their 10-year beta's derived by Morningstar's capital asset pricing model.

[7] A financial return that does not take into consideration reinvestment of dividends. Dividends are treated as a cash payout as of the end of the period. The calculation is point to point using adjusted price at the beginning of the period and the adjusted price at the end of the period incorporating any dividends paid.

[8] Data Privacy and Security Management Scores prior to incident; Score 75 to 100 (12), Score of 25 to 50 (18), Score of 0 or N/A (38).

[9] A financial return that does not take into consideration reinvestment of dividends. Dividends are treated as a cash payout as of the end of the period. The calculation is point to point using adjusted price at the beginning of the period and the adjusted price at the end of the period incorporating any dividends paid.

[10] The Legal Data Privacy and Security Management Scores prior to incident; Score 75 to 100 (12), Score of 25 to 50 (18), Score of 0 or N/A (38).

[11] A financial return that does not take into consideration reinvestment of dividends. Dividends are treated as a cash payout as of the end of the period. The calculation is point to point using adjusted price at the beginning of the period and the adjusted price at the end of the period incorporating any dividends paid.

[12] A statistical measurement of dispersion about an average and depicts how widely the returns varied over a certain period of time. Morningstar computes standard deviation using the trailing monthly total returns for the appropriate time period. All of the monthly standard deviations are then annualized.

[13] Fernando, J et. al. "Compound Annual Growth Rate (CAGR) Formula and Calculation"; Investopedia (2022); accessed (19.09.2022) at: https://www.investopedia.com/terms/c/cagr.asp