Cybersecurity factors powered by BitSight

February 2018

Research Signals

Chief financial officers rate hacking the top external risk in a recent survey, with good reason. High profile cybersecurity attacks dominated the news cycle in 2017, including the Equifax data breach, the NotPetya worm, and the breach of the Securities and Exchange Commission's Edgar system, housing financial reports and other public company statements. Given the pervasiveness of cyber risks, we have partnered with BitSight Technologies to introduce factors derived from their Security Ratings that quantify cybersecurity risks to enhance stock and portfolio risk management.

- BitSight captures company-specific cybersecurity risk through a proprietary process, providing quantifiable Security Ratings
- We find BitSight Security Ratings are predictive of data breach events, and such events on average have a negative impact on excess stock price returns of 44 bps over the first 10 days from when a breach is identified
- In addition to the normalized systematic BitSight Rating and their underlying related vectors that provide transparency, we construct 16 derived factors measuring changes in ratings and industry-relative positioning, among others

Contacts

Research Signals · research-signals@markit.com

IHS Markit™

Introduction

Data breaches can cause significant damage to companies' finances and brand reputation resulting in revenue loss and customer churn, according to a recent study of 113 afflicted companies, ultimately impacting the stock price with an average decline of 5% the day a breach was disclosed. Corbet and Gurdgiev's (2017) investigation of 819 observed incidents of cybercrime further confirms increased stock price volatility particularly for cyber events in the form of hacking, larger data breaches and smaller market capitalizatoin firms, while Rosati et al. (2017) found increased bid-ask spreads and trading volume the day of 74 sampled data breach announcements.

The US Treasury's Office of Financial Research, in their 2016 Financial Stability Report, "ranked vulnerability to malicious cyber activity as a top threat with substantial potential impact" for financial institutions. However, according to the SEC rule regarding disclosure obligations relating to cybersecurity risks and cyber incidents, "To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, registrants should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary."

Outside of the US, regulators are taking aim at how companies protect personal information and disclose breaches, and are penalized for breaches with the EU's General Data Protection Regulation (GDPR) regulation, effective May 25, 2018. The aim of the GDPR is to protect citizens from privacy and data breaches by harmonizing data privacy laws across Europe and reshaping the way companies approach data privacy. The regulation's broad territorial scope means the regulation is applicable in any case where data on EU citizens is collected, whether or not the company is based in the EU.

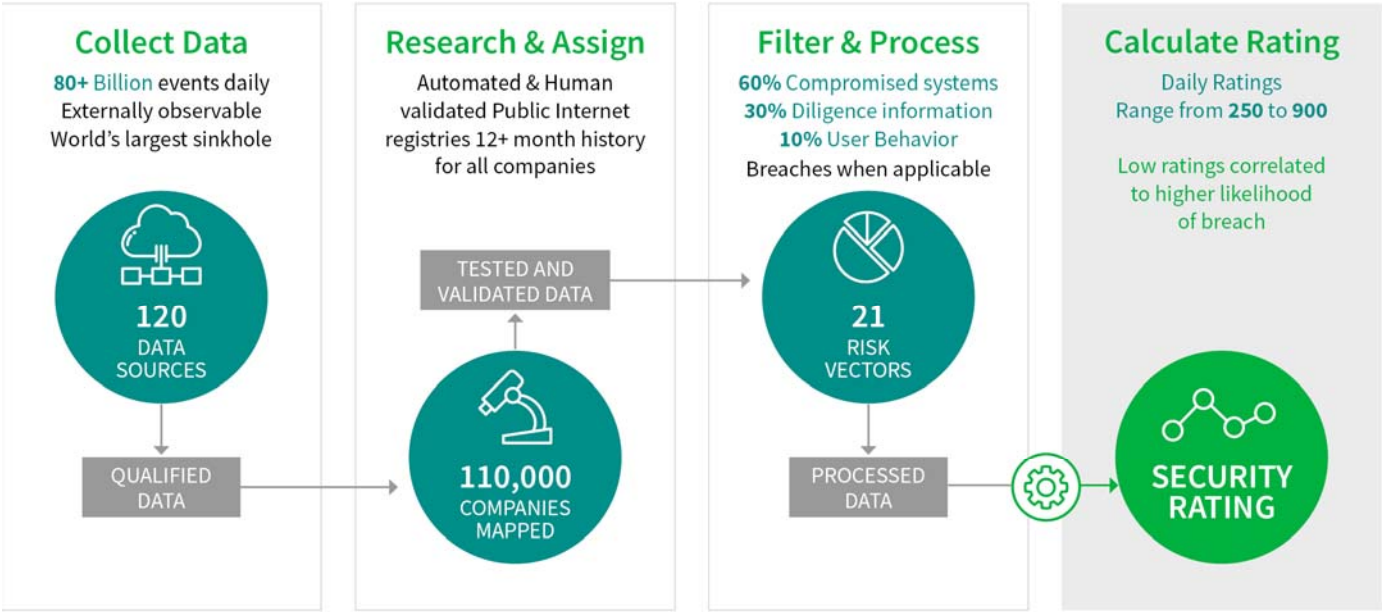
The ubiquitousness of cyber risks and the current regulatory environment expose the need for a sophisticated measurement of cyber risk. In 2011 BitSight Technologies pioneered the security ratings market, providing Security Ratings that are objective, verifiable and actionable on tens of thousands of companies worldwide. The normalized systematic measurements quantify a company's security performance to produce daily security ratings ranging from 250 to 900, with a higher rating indicating better security performance.

The remainder of this report describes our research of the BitSight security ratings and our cybersecurity factor suite. We begin by defining the dataset used in the study and our proprietary factors derived from the data. Next, we demonstrate the ability of BitSight Ratings to predict data breach events and the impact of such events on stock returns. We then turn to the performance characteristics and correlation of BitSight Ratings to traditional factors. We also walk through case studies where BitSight data identified cybersecurity risk prior to breach events. Finally, we introduce two applications for cybersecurity factors: assessing the cybersecurity risk of a portfolio and the use of a cybersecurity factor within a stock selection model.

BitSight data

BitSight analyzes existing security incidents and practices and applies sophisticated algorithms to produce these cybersecurity risk ratings (Figure 1).

Figure 1



Source: BitSight Technologies

More specifically, BitSight collects externally available internet data on security performance gathered from over 100 sources looking for malicious activity, social chatter, vulnerabilities and configuration diligence across the globe. With this data, BitSight produces daily Security Ratings by using a proprietary algorithm based on the following four dimensions:

- Compromised systems – captures risk from devices that are infected with malware and includes botnet, spam, malware server, potentially exploited applications and unsolicited communications
- Diligence – gauges efforts to reduce risk, including patching cadence, open ports and application security
- User behavior – assesses the behavior of users at the company, specifically file sharing
- Data breaches – measures actual data breach occurrences and is included when applicable

The final rating is a weighted average of these four main classes of data, with compromised systems representing the greatest weight. (See BitSight white paper for detailed analysis of security risk assessment.) BitSight suggests Ratings from 250-639 indicate basic cybersecurity risk mitigation, Ratings 640-739 indicate Intermediate mitigation, and 740-900 shows Advanced mitigation. BitSight Ratings are typically used to assess the cybersecurity risk of vendors, pricing cybersecurity insurance and internal monitoring. The use of the BitSight Ratings for stock selection and portfolio management is a novel application.

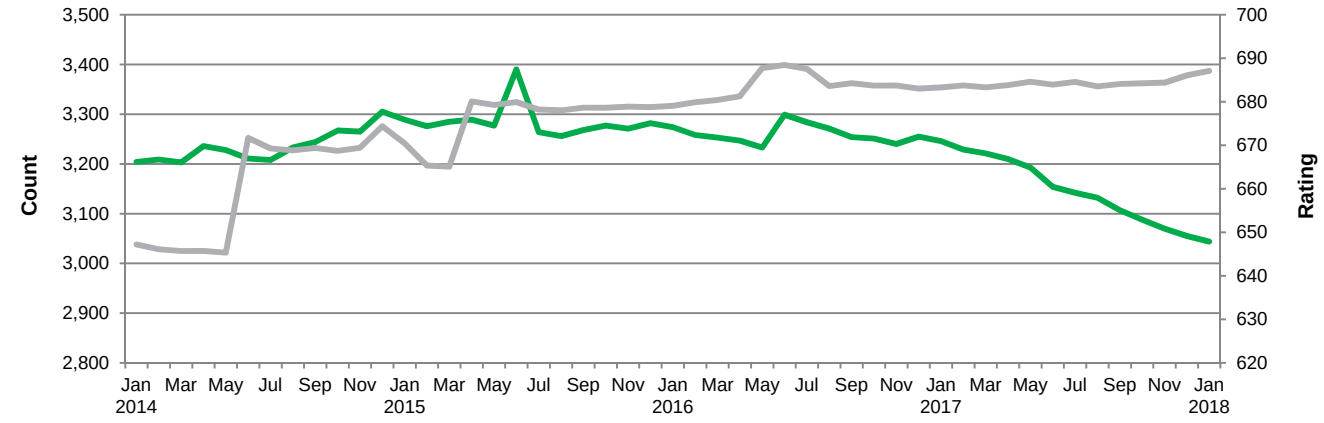
Factor introduction and descriptive statistics

Research Signals introduces a total of 35 factors in our Cybersecurity suite including the key BitSight Rating, 18 scores from the BitSight risk vectors, and 16 derived factors measuring changes and volatility in ratings, z-scores, industry and sector positioning and impact of data breaches (see the Appendix for the full list of factors and their definitions). We have mapped the data from BitSight to stock identifiers of our US Total Cap universe (98% of cumulative market cap, or approximately 3,000 names), while other regions will be covered at a later date. Thus, the data can be easily plugged into existing processes allowing for individual stock and portfolio assessment of cybersecurity risk based on a normalized systematic measure.

Coverage of the BitSight Rating factor begins in January 2014 and has averaged over 3,200 names (Figure 2). As of January 2018, coverage stands at 3,044 names. The average Rating has ranged between 645 and 688 over this period and now resides at 687.

Figure 2

BitSight Rating descriptive statistics



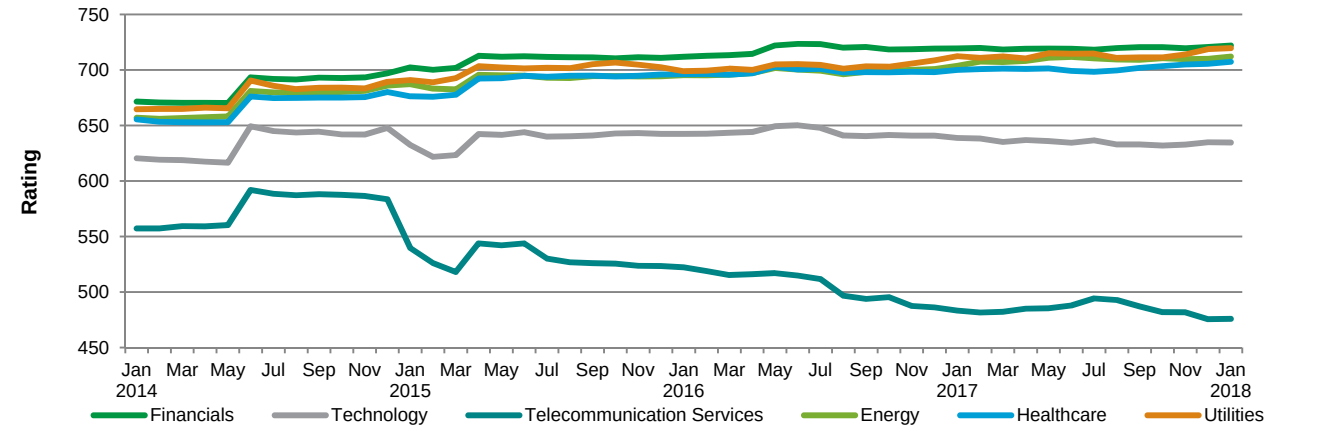
Source: IHS Markit

Taking a closer look at the distribution of BitSight Ratings, we find interesting variations between sector and industry groups (see Tables A1 and A2, respectively, in the Appendix for a complete list of average Ratings). Highlighting a few sectors of interest (Figure 3), we see that Financials have consistently scored the highest, with Banks the strongest industry subgroup, indicative of the constituents' position as having the most to lose. On the other hand, Technology and Telecommunication Services have been the weakest sectors over time, an interesting fact given that they are on the cutting edge of technology, but perhaps suggesting that their lines of business provide more opportunities to be hacked and are the hardest to protect against cyber risks. These observations indicate an industry adjustment may be warranted, which we address in our factor calculations.

The sectors which have seen the most improvement over the past year include Utilities, Healthcare and, to a certain extent, Energy. The top scoring industries include Industrials transportation subgroups, followed by Banks, Homebuilding & Construction Supplies and Renewable Energy. In addition to Technology and Telecommunication Services subgroups, other poorly scoring industries include Media & Publishing, Industrial Conglomerates, Hotels & Entertainment Services, Aeropspace & Defense and Automobiles & Auto Parts.

Figure 3

BitSight Rating sector averages

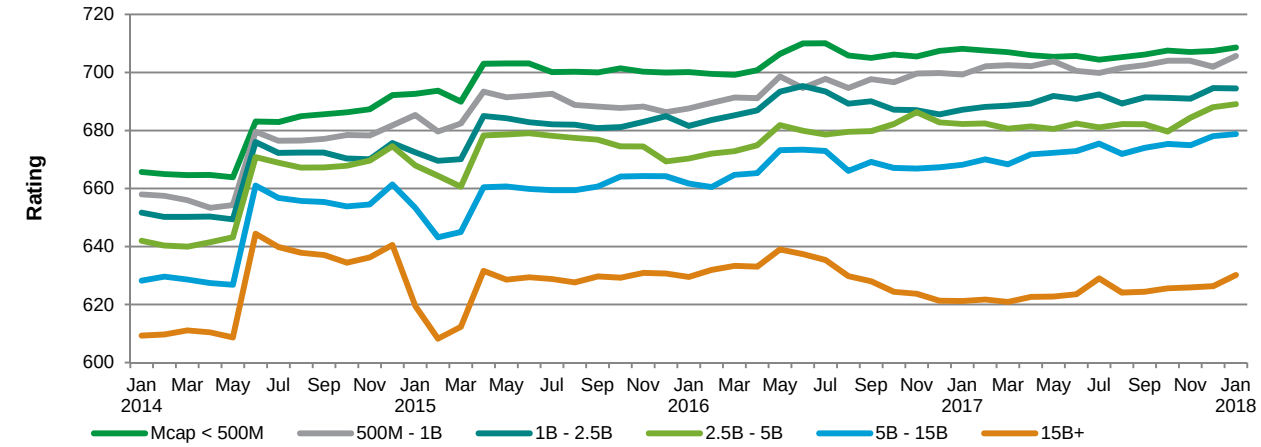


Source: IHS Markit

Lastly, we evaluate BitSight Ratings across company size, from microcaps (<$500M) to large caps (15B+). Large caps consistently have lower Ratings, averaging 627 since January 2014. Overall, Ratings tend to move inversely with market cap, indicating higher vulnerabilities as companies grow in size.

Figure 4

BitSight Rating market cap averages



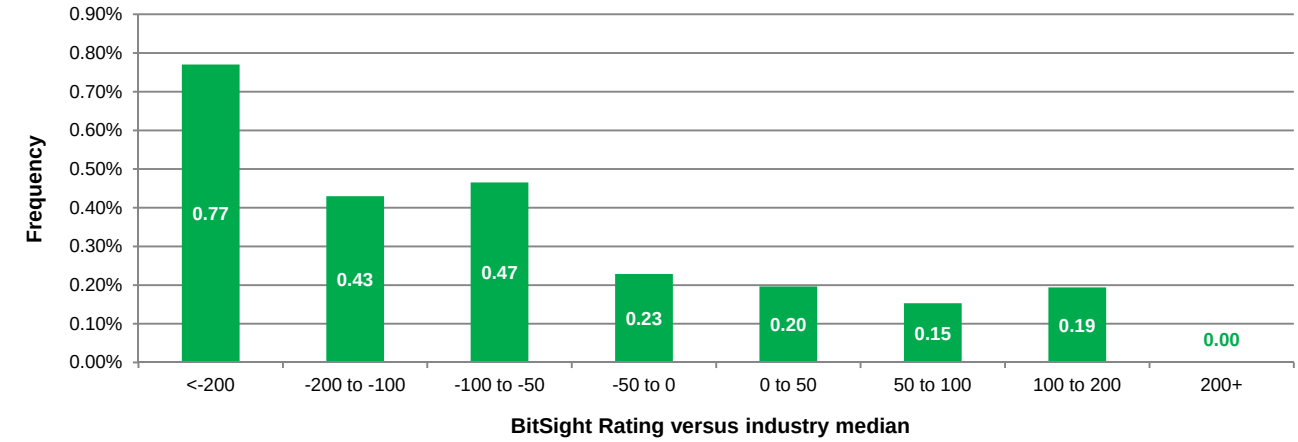
Source: IHS Markit

Data breach prediction

We now present results based on the predictability of BitSight Ratings. Two aspects are considered, namely the prediction of breach events and the implication for stock prices. Beginning with breach prediction, we compute the frequency of data breaches based on firms' BitSight Ratings relative to the industry median (Figure 5) for stocks in our investible universe. Based on our independent results, we find that, while breaches are rare overall (see Figure A1 in the Appendix for the number of breaches by quarter), firms with the weakest scores (<-200) are the most likely to experience a data breach (0.77%). The average frequency for the remaining groups registering below the industry median is 0.37% compared with 0.18% in the 0 to 200 range, while no breaches were recorded in the 200+ group. These findings corroborate BitSight's research on the ability of the BitSight Rating to predict data breaches on public and private companies.

Figure 5

Data breach frequency for industry-relative BitSight Ratings, Jan 2014 - Sep 2017



Source: IHS Markit

Turning to stock price movement around the time of data breaches, we perform an event study of the occurrences that took place during our analysis period. We report average BitSight Ratings and average Rating versus the industry median for the 527 breaches in our universe, along with excess returns over various horizons starting from the day the breach was added to the database (Table 1). Results are broken out by severity level, where 0 severity indicates a breach occurred but 0 records were lost, 1 indicates 1-10 records were lost, 2 indicates between 11 and 100,000 records were lost, and 3 is the most severe, meaning that >100,000 records were affected by the data breach.

In general, we find that excess returns tend to decline over the first 10 days subsequent to a data breach and then revert up after that period. The weakest 10-day excess returns are associated with severity classifications of 2 and 3, with average 10-day excess returns of -0.818% and -0.434%, respectively, while both recover at the 20-day horizon (1.388% and 0.918%, respectively). Conversely, excess returns for the lowest severity breaches remain positive over each horizon.

Table 1

Data breach occurrences, Jan 2014 – Sep 2017

Severity	Count	Average BitSight Rating	Average distance from industry median	Average 5-day excess return	Average 10-day excess return	Average 15-day excess return	Average 20-day excess return
All	527	630	-64.5	-0.099%	-0.442%	-0.044%	1.689%
0	172	625	-80.9	0.136%	0.190%	1.242%	3.746%
1	37	630	-53.1	-0.221%	-0.068%	-0.391%	-0.284%
2	286	638	-55.7	-0.294%	-0.818%	-0.422%	1.388%
3	32	593	-68.3	-0.382%	-0.434%	-0.324%	0.918%

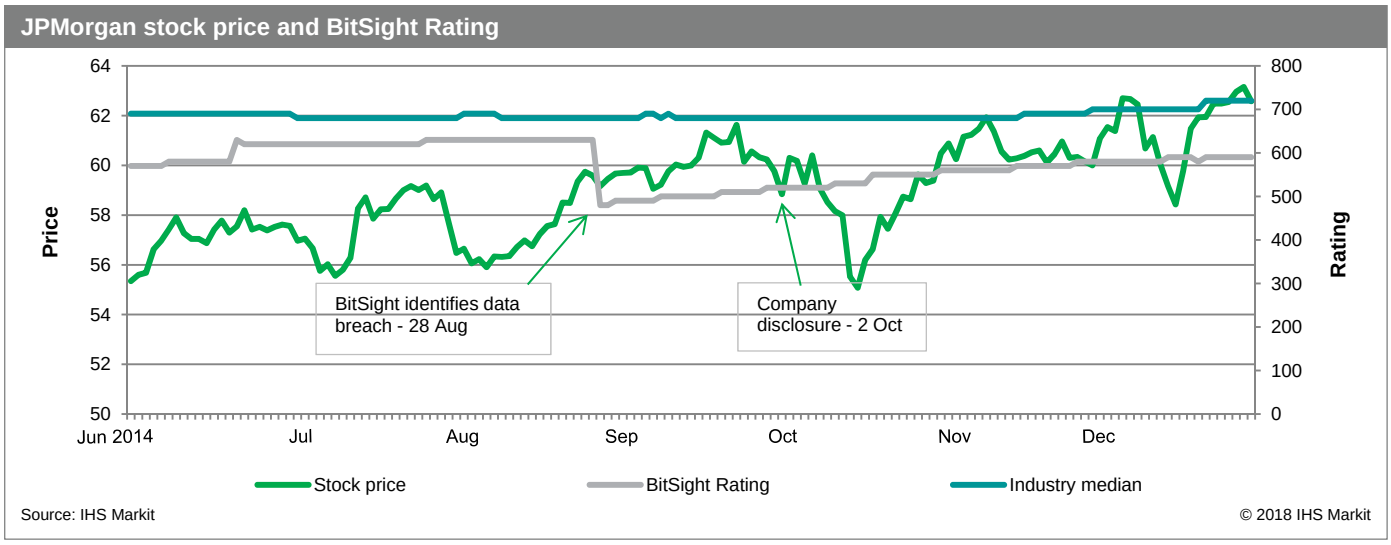
Source: IHS Markit

Next, we provide several case studies demonstrating application of the BitSight Rating including JPMorgan, Mondelez and Equifax.

JP Morgan

In late August 2014, it was reported that the FBI was investigating cyberattacks at JPMorgan Chase and six other top banks (Figure 6). The hack was expected to have the potential to delete and manipulate records in customer bank accounts and investor accounts; however, the bank denied that any unusual activity was detected. Yet, JPMorgan did not officially file Form 8-K with the SEC until October 2nd 2014 updating information regarding the extent of the previously disclosed cyberattack. The form is used to announce material corporate events that shareholders should know about on a more current basis beyond annual Form 10-Ks and quarterly Form 10-Qs. In this case, the company disclosed that user contact information and internal bank information of approximately 76 million households and 7 million small businesses was impacted. BitSight identified the data breach and downgraded its score 24 trading days prior to the company disclosure.

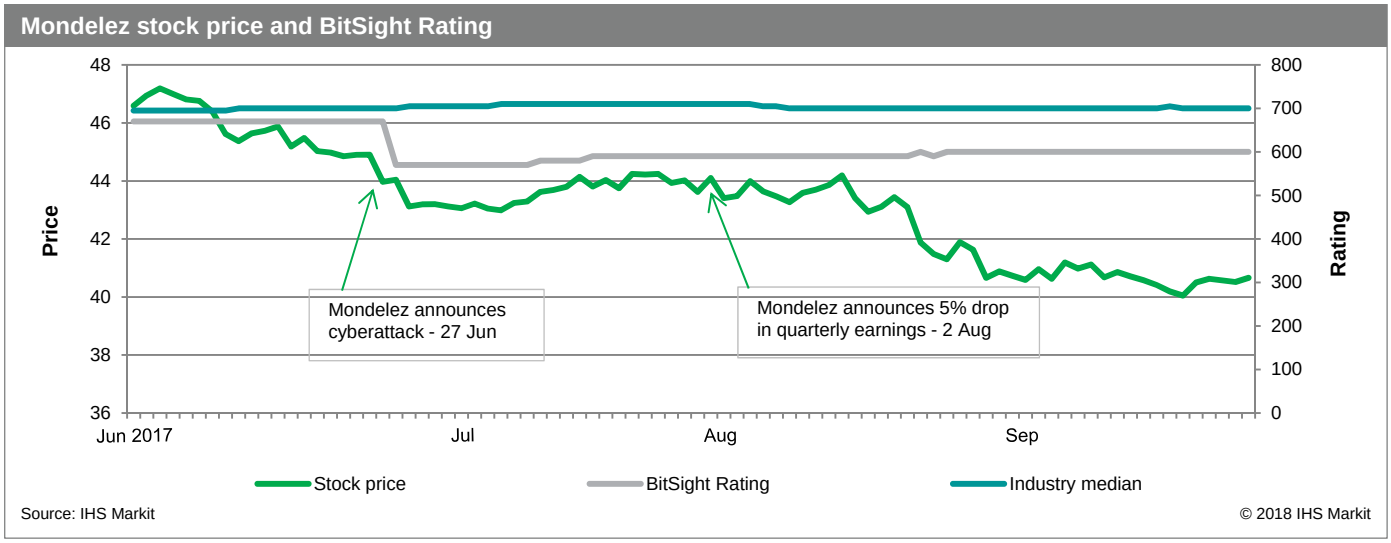
Figure 6



Mondelez

Mondelez International, a worldwide manufacturer of snack foods and beverages formerly known as Kraft Foods Inc, was one of several companies impacted by a cyberattack on 27 June 2017, known as NotPetya. Some of the world's biggest companies suffered computer outages affecting corporate earnings due to loss of sales or production. Mondelez announced a 5% drop in quarterly earnings on 2 August, citing shipping and invoice delays caused by the attack. BitSight's Rating reacted to the initial "worm" attack 25 trading days prior to the earnings disappointment.

Figure 7



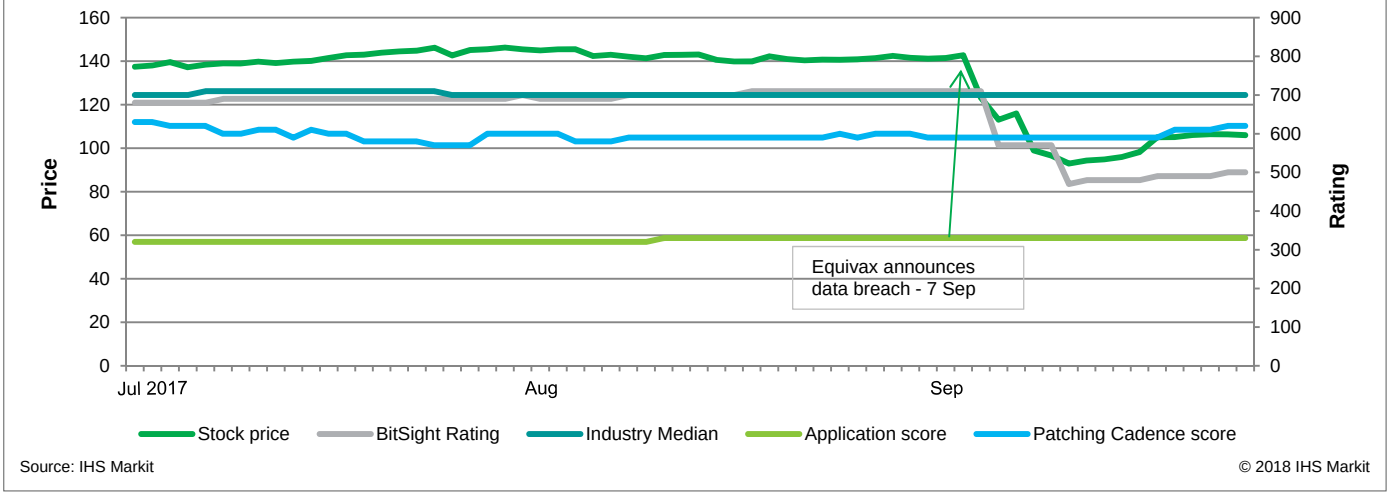
Equifax

In perhaps one of the most infamous cyberattacks, in mid-May 2017, hackers gained access to the systems of Equifax, one of three major credit reporting agencies, potentially exposing the personal information, including names, social security numbers, birth dates and driver's license numbers of more than 143 million consumers. However, the breach was not discovered until July 29th and the company did not report the incident until September 7th (Figure 8). Equifax's BitSight Rating prior to the announcement was almost identical to the industry median. After the announcement, we see two sharp drops in the BitSight Rating as the data breach was first announced, followed by a subsequent announcement that the breach was broader than first indicated. We also include 2 underlying risk factors, Application Security and Patching

Cadence, to highlight that risk associated with securing applications from external hacking was a risk identified prior to the announcement.

Figure 8

Equifax stock price and BitSight Rating



Source: IHS Markit

Factor performance and correlation

Next we turn to factor attribution, beginning with analysis of factor performance. We report the spread between top (decile 1) and bottom (decile 10) rated stocks for the key underlying BitSight Rating factor along with Industry Relative BitSight Rating given our previous findings (Table 2). Various holding periods are considered including 1-, 3-, 6- and 12-month horizons from January 2014 through January 2018 on both a cross sectional and sector neutral basis.

Table 2

Factor decile return spread performance, Jan 2014 – Jan 2018

	BitSight Rating		Industry Relative BitSight Rating	
Holding period	**Cross sectional**	**Sector neutral**	**Cross sectional**	**Sector neutral**
1-month	-0.09	-0.08	-0.13	-0.05
3-month	-0.06	-0.24	-0.17	0.07
6-month	-0.43	-0.46	-0.88	-0.32
12-month	-0.96	-0.22	-0.68	-0.33

Source: IHS Markit

Factor performance for both factors across the various holding periods tended to be inconsistent over time resulting in relatively flat spreads. For 1-month holding periods, the average cross sectional spread was -0.09 (-9 bps) for BitSight Rating, similar in level based on industry relative construction (-0.13), and spreads came in at -0.96 and -0.68, respectively, at the 12-month horizon. As one might expect, while cybersecurity is an important risk to measure, these findings suggest that it is not a standalone driver of stock returns on a cross-sectional basis.

Beyond absolute performance, we also look for diversifying features offered from BitSight Rating relative to other alpha factors. For this perspective, we use factors from our Consolidated Factor library, offering broad representation across styles. Analysis is based on two aspects of factor correlation, including Information Coefficient (IC) correlation for 1-month holding periods and average factor rank correlations (see Table A3 in the Appendix).

The highest BitSight Rating IC correlation is associated with Natural Logarithm of Market Capitalization (0.791), which also has a high rank correlation (0.232), not surprising given our previous attribution results. High IC correlations are also

realized with Implied Volatility (0.624), Book-to-Market (0.563) and Slope of 3-yr TTM Sales Trend Line (0.526). At the opposite extreme, Total Debt to Total Assets (-0.582), Industry Relative TTM Dividend Yield (-0.426) and Industry Relative Leading 4-QTRs EPS to Price (-0.416) demonstrated the most negative co-movement with BitSight Rating. Other factors of interest with notable rank correlations include 60-Month Beta (0.067) and Demand Supply Ratio (-0.087).

Factor application

We round out the report with examples of BitSight Rating applications. First, in order to gain alternative insights into portfolio risk exposures, we use BitSight Ratings to evaluate increased probabilities of cyberattacks for the holdings in a typical portfolio. In this case, we use decile rankings of our Value Momentum Analyst II (VMA2) model, a comprehensive multi-factor approach including factors that span value, quality, price and earnings momentum styles. We report average BitSight Ratings and the average distance from the industry median across deciles on 31 January 2018 (Table 3).

For this portfolio application, we find that the highest ranked decile 1 names have a high average BitSight Rating of 697 and an average distance below the industry median of just 9.9. However, the most poorly ranked decile 10 names are further associated with a relatively low average BitSight Rating of 671 and an average distance from the median of 43.4, suggesting that additional attention may need to be paid to this cohort of unfavorably ranked names.

Table 3

VMA2 BitSight Rating exposures, Jan 2014 – Jan 2018

Decile	Average BitSight Rating	Average distance from industry median BitSight Rating
1	697	-9.9
2	689	-15.2
3	689	-28.4
4	699	-13.8
5	686	-25.2
6	684	-22.4
7	665	-33.0
8	713	-7.2
9	653	-56.3
10	671	-43.4

Source: IHS Markit

In our second application, we aim to incorporate cybersecurity risk measures into a multifactor stock selection model. We again begin with VMA2 and overlay it with Industry Relative BitSight Rating using a 10% weighting, while assigning the remaining 90% weighting to the base model. We compare performance of the combined model with the stand alone model based on top versus bottom decile return spreads (Table 4) using our Total Cap universe.

While VMA2 has a strong proven track record, the BitSight overlay enhances returns over the analysis period. The average spread for the combined strategy was 1.21% compared with 1.15% for the base model, with a modest reduction in volatility (standard deviation: 3.09 vs 3.19). On a cumulative basis (Figure 9), the addition of Industry Relative BitSight Rating added 5.4 percentage points of return. Benefits were particularly seen from identifying higher risk names, as the overlay methodology posted a deeper average downside for sell-rated (D10) names of -0.72% per month, compared with -0.62% for VMA2.

Table 4

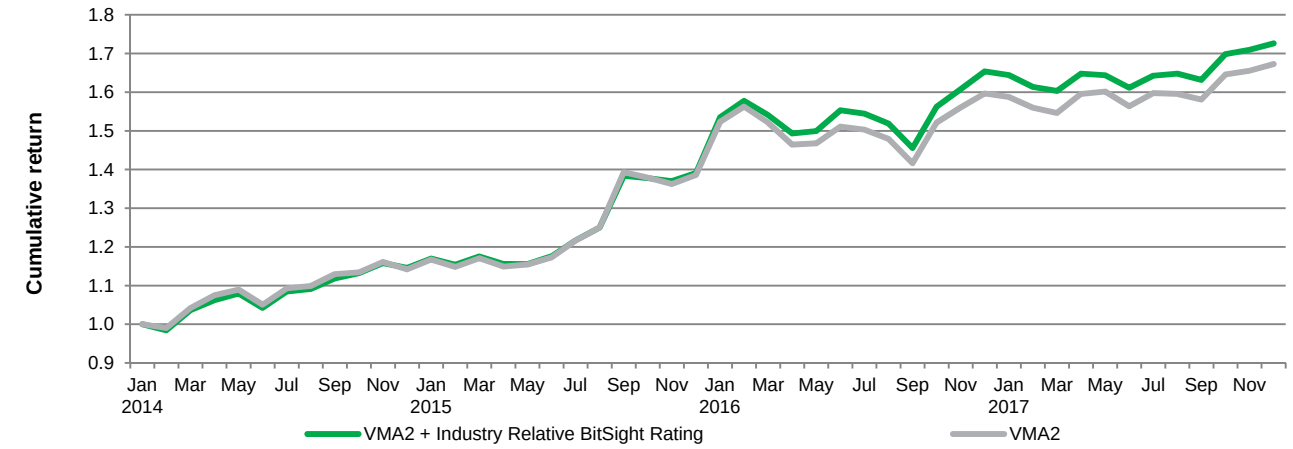
VMA2 model performance, Jan 2014 – Jan 2018

	VMA2 + Industry Relative BitSight Rating			VMA2		
	Decile spread	D1 excess return	D10 excess return	Decile spread	D1 excess return	D10 excess return
Average	1.21%	0.49%	-0.72%	1.15%	0.52%	-0.62%
Standard deviation	3.09	1.20	2.12	3.19	1.22	2.20
Hit rate	60%	72%	36%	62%	70%	38%
IR	0.39	0.41	-0.34	0.36	0.43	-0.28

Source: IHS Markit

Figure 9

VMA2 + Industry Relative BitSight Rating cumulative decile spread performance



Source: IHS Markit

Conclusion

BitSight offers independent third party monitoring of company cybersecurity risk using a systematic approach to produce a daily Security Rating. Based on this underlying score, we introduce 16 derived factors in addition to 19 factors passed through directly from BitSight. We have mapped the BitSight data across our US Total Cap universe (3,000+ names), allowing the stock-specific data to easily plug into existing processes to assess individual stocks and portfolios with a normalized systematic measure of cybersecurity risk.

BitSight Ratings range from 250 to 900, with a higher rating indicating better security performance, and average between 645 and 688 from January 2014 through January 2018. Financials have consistently scored the highest, with Banks the strongest industry subgroup, while Technology and Telecommunication Services have been the weakest sectors over time. Ratings also tend to move inversely with market cap.

While BitSight Technologies had an independent third party confirm the Ratings predictability of breaches, we conducted our own analysis showing that BitSight Ratings are predictive of data breach events. While breaches are rare overall, firms with the weakest scores relative to the industry median (<-200) are the most likely to experience a data breach at a frequency of 0.77%, compared with 0.18% in the 0 to 200 range and no breaches in the 200+ group. Data breach events are also found to typically lead to negative returns relative to the market, particularly in the first 10 days after the event, before subsequently reverting up. We include case studies for JPMorgan, Mondelez and Equifax, where notable breaches were identified prior to public announcements of the financial impact.

In terms of factor performance, BitSight Rating results across various holding periods tended to be inconsistent over time resulting in relatively flat decile spreads. However, the factor offers diversification relative to other alpha factors such as Total Debt to Total Assets, Industry Relative TTM Dividend Yield and Industry Relative Leading 4-QTRs EPS to Price.

Lastly, we demonstrate application of the Ratings in a portfolio setting. Using our proven multi-factor style model, VMA2, we find an average BitSight Rating of 697 for buy-rated (D1) names, compared with 671 for sell-rated (D10) names, highlighting an additional source of potential risk exposure. A methodology of overlaying Industry Relative BitSight Ratings with the base model also resulted in 5.4 percentage points of additional return for cumulative spreads over the analysis period, particularly from identifying sell-rated names with weaker average returns.

Appendix

Cybersecurity factor suite

BitSight factors

- BitSight Rating – calculated using a proprietary algorithm that analyzes and classifies externally observable data, with scores ranging from 250 to 900, where higher ratings indicate more effective company implementation of good security practices
- Botnet Risk – a unified network of machines that are performing coordinated actions based on instructions received from the malware's creators
- Malware Server Risk – a machine hosting a website that injects malicious code into a visitor's browser, often resulting in the installation of new malware on that visitor's computer
- Potentially Exploited Software Risk – a machine running a potentially unwanted application which leaves the system vulnerable to adware, spyware, and remote access tools
- Spam Propagation Risk – machines compromised with malware that causes them to send large volumes of unwanted email
- Unexpected Communications Risk – any host that is observed trying to contact a service on another host that is not expected or supported
- Domain Keys Identified Mail (DKIM) Risk – a protocol designed to prevent unauthorized servers from sending email on behalf of a company's domain
- Sender Policy Framework (SPF) Risk – a DNS (Domain Name System) record identifying which mail servers are permitted to send email on behalf of a domain, preventing spammers from sending emails with forged "From:" addresses
- TLS/SSL Configuration – records indicating that servers have properly configured security protocol libraries and support strong encryption standards when making encrypted connections to other machines
- TLS/SSL Certificates – records verifying the authenticity of your company servers to your associates, clients, and guests, and which serve as the basis for establishing cryptographic trust
- DNSSEC Records – a protocol that uses public key encryption to authenticate DNS servers
- Open Ports – ports that are exposed to the public internet, which are evaluated to determine whether or not unnecessary access points exist

- Application Security – HTTP header configurations that inform how to receive and respond to web requests in a manner that prevents malicious behavior such as man-in-the-middle and cross-site scripting attacks
- User Behavior – examines activities that may introduce malicious software onto a corporate network, for example, by downloading a compromised file
- Patching Cadence – the speed at which a company resolves publicly disclosed vulnerabilities, which are bugs in software or device firmware that can be used to gain unauthorized access to systems and data
- Insecure Systems – shows which endpoints inside an organization are communicating with an unintended destination. The software in these endpoints have been tampered with or misconfigured, and end up communicating with a remote server that, if captured, may allow attackers to inject code, breach the organization, or extract sensitive data.
- Desktop Software – desktop software are laptops, servers, and other non-tablet, non-phone computers in a company's network which access the internet. If there are unsupported desktop software in an organization's network, there is a greater risk of system failure (vendor devices are not being maintained), disruption of business continuity, and attackers may be able to use unpatched vulnerabilities to gain system access.
- Mobile Software – mobile software are smartphones and tablets in a company's network which access the internet. If there are unsupported mobile software in an organization's network, there is a greater risk of system failure (vendor devices are not being maintained), disruption of business continuity, and attackers may be able to use unpatched vulnerabilities to gain system access.
- Server Software – this risk type can be used to create a rich picture about the software used by an organization. It helps track security holes created by server software that is no longer supported by its original developers or has become out-of-date (deprecated).

Research Signals derived factors

- 1-Week Change in BitSight Rating – change in BitSight Rating over the past 1 week
- 1-Month Change in BitSight Rating – change in BitSight Rating over the past 1 month
- 3-Month Change in BitSight Rating – change in BitSight Rating over the past 3 Months
- 12-Week Volatility in BitSight Rating – standard deviation of the BitSight Rating over the past 12 weeks
- BitSight Rating 8-week Z-score – z-score of the BitSight Rating over the past 8 weeks, calculated as the current rating of a company minus the average rating for the past 8 weeks, divided by the standard deviation over the past 8 weeks (if standard deviation is 0, the z-score is 0)
- BitSight Rating 12-week Z-score – z-score of the BitSight Rating over the past 12 weeks, calculated as the current rating of a company minus the average rating for the past 12 weeks, divided by the standard deviation over the past 12 weeks (if standard deviation is 0, the z-score is 0)
- BitSight Rating 26-week Z-score – z-score of the BitSight Rating over the past 26 weeks, calculated as the current rating of a company minus the average rating for the past 26 weeks, divided by the standard deviation over the past 26 weeks (if standard deviation is 0, the z-score is 0)
- BitSight Rating 52-week Z-score – z-score of the BitSight Rating over the past 52 weeks, calculated as the current rating of a company minus the average rating for the past 52 weeks, divided by the standard deviation over the past 52 weeks (if standard deviation is 0, the z-score is 0)

- Distance from Industry Median BitSight Rating – difference between the company's current BitSight Rating and the median BitSight Rating for the industry
- Industry Relative BitSight Rating – difference between the company's current BitSight Rating and the average BitSight Rating for the industry, scaled by the standard deviation of the industry's BitSight Ratings
- Distance from Sector Median BitSight Rating – difference between the company's current BitSight Rating and the median BitSight Rating for the sector
- Sector-Relative BitSight Rating – difference between the company's current BitSight Rating and the average BitSight Rating for the sector, scaled by the standard deviation of the sector's BitSight Ratings
- Compromised Systems Score – score penalizing companies with poor observed compromised systems risk. It is calculated as the minimum of the risk scores in the diligence category, which includes Botnet Risk, Malware Server Risk, Potentially Exploited Software Risk, Spam Propagation Risk, and Unexpected Communications Risk.
- Diligence Score – score penalizing companies with poor observed cybersecurity diligence. It is calculated as the minimum of the risk scores in the diligence category, which includes Sender Policy Framework (SPF) Risk , Domain Keys Identified Mail (DKIM) Risk, TLS/SSL Certificates, TSL/SSL Configuration, Open Ports, Application Security, and Patching Cadence.
- Data Breach Impact – score penalizing companies with data breaches within the past 1 year. More recent and severe data breaches have greater negative impact on this score.
- Data Breach Relevance – score penalizing companies with data breaches within the past 1 year. More recent data breaches have greater impact on this score.

Tables and figures

Table A1

Average BitSight Rating, Jan 2014 – Jan 2018

Sector	Average Rating
Basic Materials	679
Cyclical Goods & Services	659
Energy	693
Financials	708
Healthcare	689
Industrials	670
Non-Cyclical Goods & Services	679
Not Defined	719
Technology	638
Telecommunication Services	523

Source: IHS Markit

Table A2

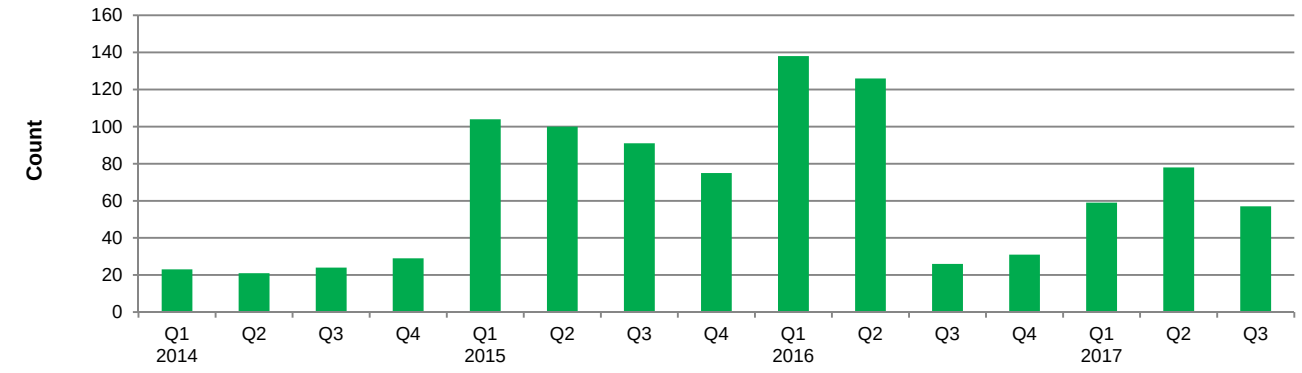
Average BitSight Rating, Jan 2014 – Jan 2018

Industry group	Average Rating
Basic Materials	
Containers & Packaging	665
Paper & Forest Products	677
Chemicals	678
Construction Materials	689
Metal & Mining	682
Cyclical Goods & Services	
Automobiles & Auto Parts	655
Homebuilding & Construction Supplies	720
Homebuilding & Household Goods	682
Textiles & Apparel	696
Hotels & Entertainment Services	643
Media & Publishing	626
Retailers	675
Energy	
Coal	702
Energy Related Equipment & Services	680
Oil & Gas	698
Renewable Energy	715
Financials	
Banks	722
Financial Services - Diversified	685
Holding Companies	719
Insurance	703
Collective Investments	696
Real Estate	684
Real Estate Operations	700
Healthcare	
Biotechnology & Medical Research	663
Biotechnology & Pharmaceuticals	700
Healthcare Equipment & Supplies	674
Healthcare Providers & Services	668
Industrials	
Industrial Conglomerates	633
Aerospace & Defense	654
Industrial Machinery & Equipment	662
Commercial Services & Supplies	674
Construction, Engineering & Materials	681
Diversified Trading & Distributing	696
Air Freight & Courier Services	667
Airline Services	680
Freight & Logistics Services	727
Marine Services	693
Passenger Transportation Services	780
Rails & Roads Transportation	666
Non-Cyclical Goods & Services	
Beverages	683
Food & Tobacco	678
Food & Drug Retailing	698
Personal & Household Products & Services	668
Technology	
Software & IT Services	647
Communications Equipment	593
Computers & Office Equipment	621
Computers, Phones & Household Electronics	676
Semiconductors	638
Telecommunications Services	
Telecommunications Services	523
Utilities	
Electric Utilities	694
Gas Utilities	707
Utilities - Multiline	693
Utilities - Water & Others	713

Source: IHS Markit

Figure A1

Number of data breaches by quarter



Source: IHS Markit

Table A3

BitSight Rating correlations, Jan 2014 – Jan 2018

Factor	1-month IC correlation	Average Rank Correlation
Natural Logarithm of Market Capitalization	0.791	0.232
Implied Volatility	0.624	0.168
Book-to-Market	0.563	0.113
Slope of 3-yr TTM Sales Trend Line	0.526	0.076
Asset Quality Index	0.494	0.026
2-Year Ahead EPS Growth	0.320	-0.008
Working Capital Accruals	0.258	0.003
Average Monthly Trading Volume-to-Market Cap	0.223	0.065
4-Quarter Sales Acceleration	0.156	-0.007
Put/Call Ratio	0.140	0.015
Fixed Assets Turnover Ratio	0.121	-0.024
TTM Free Cash Flow-to-Enterprise Value	0.105	-0.056
5-day Industry Relative Return	0.082	0.005
Change in Accruals to Assets	0.044	-0.006
Altman Z Score	-0.029	-0.054
Real Earnings Surprise	-0.041	-0.011
Forward 12-M EPS-to-Enterprise Value	-0.043	-0.066
TTM EBITDA-to-Enterprise Value	-0.062	-0.061
Inventory Turnover Ratio	-0.093	-0.046
Rational Decay Alpha	-0.104	-0.005
Net Operating Asset Turnover	-0.135	-0.120
3-M Revision in FY2 EPS Forecasts	-0.142	0.007
Implied Loan Rate	-0.156	-0.070
Change in TTM Sales vs. Accounts Receivable	-0.180	0.014
1-yr Growth in TTM Free Cash Flow	-0.184	-0.067
Operating Leverage	-0.212	-0.013
Change in TTM COGS vs. Inventory Level	-0.217	-0.077
60-Month Beta	-0.224	0.067
Demand Supply Ratio	-0.229	-0.087
24-Month Value at Risk	-0.257	-0.045
Reinvestment Rate	-0.327	-0.082
Industry-adjusted 12-month Relative Price Strength	-0.341	-0.038
Net External Financing	-0.408	-0.102
Industry Relative Leading 4-QTRs EPS to Price	-0.416	-0.099
Industry Relative TTM Dividend Yield	-0.426	-0.055
Total Debt to Total Assets	-0.582	-0.131

Source: IHS Markit

References

Corbet, Shaen and Constantin Gurdgiev (2017). “What the Hack: Systematic Risk Contagion from Cyber Events”. Working paper.

Rosati, Pierangelo, Mark Cummins, Peter Deeney, Fabian Gogolin, Lisa van der Werff and Theo Lynn (2017). “The effect of data breach announcements beyond the stock price: Empirical evidence on market activity”. Internatinal Review of Financial Analysis, Volume 49, Januaary 2017, pages 146-154.

IHS Markit Customer Support:

Support@markit.com
Americas: +1 877 762 7548
Europe, Middle East, and Africa: 00800 6275 4800
Asia and the Pacific Rim: +65 6922 4210