TEMATICARESEARCH®

Cybersecurity & Data Privacy - Global Classification

Version 5.0
Dated 14 November 2019

About Us

Tematica Research, LLC ("**Tematica**") provides independent Registered Investment Advisors (RIAs), financial institutions and self-directed investors with equity research, economic insights, and investment ideas based upon its proprietary thematic perspective of the world and financial markets.

At the core of everything Tematica does is the company's thematic lens, which has given rise to Tematica's investment themes. The investment themes are identified by looking at the intersection of shifting economics, demographics, psychographics and technologies, mixed in with regulatory mandates and other forces. Such thematic shifts cut across sectors and tend to result in major structural changes and disruptions to behaviours and business models.

Our thematic research process aims to identify those companies poised to leapfrog ahead of the competition, riding the tailwinds from one or more of these themes.

1. Tematica's approach to thematic investing

Thematic investing is exactly what it sounds like: making investment decisions based upon enduring themes. Tematica's investment themes are identified by looking at the intersection of shifting economics, demographics, psychographics and technologies, mixed in with regulatory mandates and other forces to identify sustainable and structural market shifts. These shifts shape and impact consumer behavior and, in turn, force companies to make fundamental changes to their businesses in order to succeed.

Some companies will adapt and survive (Coca-Cola Co.), a few will embrace the change more fully and leapfrog ahead of the pack (Netflix moving away from DVDs to a streaming subscription business model) while others will utterly upend the way things have always been done (Amazon) and then there are those new entrants that shake everything up (DocuSign), riding these thematic tailwinds to profits while enjoying significant share price gains. Some will sadly be left floundering as they entirely misread the changing thematic winds and become irrelevant (Kodak).

The process Tematica utilizes to analyze and assess the impact of its investment themes on a company's business model produces an enormous amount of data —

data that can be licensed in the form of the Thematic Scorecard or through several Thematic Indices that have been created.

1.1. Thematic Scorecard: What is it and how is it used?

The Thematic Scorecard ("**Scorecard**") is the database maintained by Tematica of individual stocks that have been thematically scored across Tematica's investment themes. This thematic universe of securities is compiled using screening tools and is updated once in the first half of the calendar year, and once in the second half of the calendar year.

Included are global publicly-listed companies trading on major international exchanges that meet the following criteria as of the last trading day of the month prior to compilation:

- Market Capitalization of $250 million and over
- Share Price greater than or equal to $10
- 30-day Trading Volume greater than or equal to 100,000 shares

The Scorecard is utilized by Tematica through its published research, economic commentary and in the construction of its custom indices.

As of July 2019, the Scorecard contained approximately 3,000 public companies.

1.2. How are stocks thematically scored?

The Scorecard contains levels of scores that represent the extent of a company's exposure to one or more investment themes. Each company's exposure to an investment theme is determined using publicly available data provided by the company through 10-Ks, 10-Qs, 20-Fs, 8-Ks and other SEC or similar filings, quarterly earnings reports, company presentations or official earnings conference call transcripts.

A company's thematic exposure is measured by the percentage of operating profit influenced by the tailwinds or headwinds generated from each theme. If operating profit isn't available, reported net sales data, either through official filings, transcripts or company presentations, is utilized as a proxy for exposure. If, in analyzing a company's public materials, it is clear that its operations are benefiting from a theme, but no specific revenue or operating profit data is reported that can verify the extent to which the company is benefiting from the theme, the company receives a Level 1 score for its thematic exposure.

Level 1	The company has peripheral exposure to the theme, no specific revenue or operating profit data is reported that can verify the extent to which the company is benefiting from the theme
Level 2	The company generates between 20% and 50% of its reported revenue or operating profit from the theme
Level 3	The company generates between 50% and 80% of its reported revenue or operating profit from the theme

Level 4	The company generates over 80% of its reported revenue or operating profit from the theme
Level 5	The company generates close to 100% of its reported revenue or operating profit from the theme

If a constituent or prospective constituent company (or professional advisor acting on behalf of the company) wishes to challenge its Thematic Scorecard score, supporting evidence should be sent to customerservice@tematicaresearch.com. The reasons for proposing a change of the company's thematic score should be stated with documentary evidence in support of its claim submitted. In considering the claim, Tematica may only take account of publicly available information.

Any adjustment resulting from a change in a company's Thematic Scorecard score will be effective in line with the next semi-annual Scorecard review. In certain circumstances, Tematica reserves the right to exercise discretion and apply the change sooner. Where discretion is being applied, Tematica will provide a minimum of two days' advance notice.

2. Cybersecurity & Data Privacy - Global Classification

2.1. Industry Universe

Tematica launched the Tematica Research Cybersecurity & Data Privacy Stock Universe ("**Industry Universe**") in 2019.

The Industry Universe is maintained by Tematica as a sub-segment of the Scorecard to capture the individual stocks that have been thematically scored across Tematica's "*Cybersecurity & Data Privacy"* investment theme. As of July 2019, the Industry Universe contained 103 companies.

The Industry Universe is designed to capture the full spectrum of products and services used in ***personal***, ***corporate*** and ***public*** applications. Each company's thematic score is determined by reference to its exposure to each of these applications. Please refer to Section 5.3 (*What are the business applications for Cybersecurity & Data Privacy?*) below for further information in respect of these applications.

Tematica does not accept payments from companies or third parties to include their stocks within the Industry Universe.

2.2. Classification

Within the Industry Universe, companies are classified according to the Tematica Research Cybersecurity & Data Privacy Global Classification ("**Classification**").

The Classification is a global market segmentation system for representing public companies in the Cybersecurity & Data Privacy ecosystem. The Classification is designed for the investment and research communities with the objective of identifying the companies, subsectors and business activities

of companies whose commercial models are benefiting from the structural shift toward greater Cybersecurity & Data Privacy spending globally.

Within the Classification, companies are classified according to whether they are “Product” providers or “Service” providers:

- ***Product providers*** – Cybersecurity products are defined as hardware and/or software that are installed locally (at the customer location) and, in the case of software, the majority of the computing power (processing) is provided by the end-customer. Interactions with the end-customer are generally limited to providing updates (virus definitions, software builds, updated hardware sales, etc.) An example of a company offering a product in this space is Avast plc. Their product is downloaded and installed by the customer on the customer’s computer or network. Periodic virus definition files and software updates are generally the extent of interaction between Avast plc and its customers.

- ***Service providers*** – Cybersecurity services are defined as hardware and/or software that are accessed remotely by the end-customer and, in the case of software, the majority of the computing power (processing) is provided by the service provider. Interactions with the end-customer often occur in real-time. An example of a company offering a product in this space is FireEye, whose solutions include cloud-based threat intelligence, security analytics and security automation and orchestration technologies, as well as managed security services, cybersecurity consulting and incident response offerings.

Reported publicly available revenue or profit data provided by the company through SEC filings, earnings reports, presentations or official earnings conference call transcripts determines a company’s product or service classification as defined above.

3. Review frequency

During each semi-annual scoring session, Tematica will adjust a company’s Classification in June and December as needed based on which subsector (“Product providers” or “Service providers”) provides the largest percentage of the company’s reported revenue or operating profit.

4. Oversight and governance

The Classification is maintained by the Tematica Research Classification Committee, which convenes twice per year in June and December. The Tematica Research Classification Committee also engages in regular dialogue with the Tematica Research Strategic Advisory Board.

Please visit www.tematicaresearch.com for further information.

5. Further information on Cybersecurity & Data Privacy

5.1. What is Cybersecurity?

For the purposes of the Classification, cybersecurity refers to the practice of protecting systems, networks, and programs from cyber-attacks.

These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

5.2. What is Data Privacy?

For the purposes of the Classification, data privacy is the branch of data security concerned with the proper handling of personal data. Data privacy is about ensuring that data and activities both online and those that generate data from activities in the physical world are accessible and used only by and in such ways as are permitted by the individual (i.e. the data subject). Data privacy can entail either Personally Identifying Information (PII) or non-PII information such as a site visitor's behaviour on a website.

The definition of "personal data" is based on the definition provided in Article 4(1) of the General Data Protection Regulation adopted by the European Union which is defined as "any information relating to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Companies receiving a "Data Privacy" tag within the Industry Universe are companies that have products and/or services that allow for or promote an individual's ability to control the collection, storage, internal use, dissemination or sale of their personal data.

5.3. What are the business applications for Cybersecurity & Data Privacy?

Cybersecurity & Data Privacy products and services are used and applied in a variety of personal, corporate and public applications:

Personal

This mainly pertains to data that is generated and controlled by individuals but also includes certain government-generated data controlled by individuals.

- Personal Data – This includes data-like addresses and locations (physical and virtual), financial information (bank accounts, credit cards, credit scores, online shopping accounts), government issued IDs (citizenship status, driver's license, other government IDs).

- Social Media/Online Presence/ Gaming – Social media accounts (including browsing traffic, email contents, posted contents) as well as data/chats/activity conducted on gaming platforms.

- Personal Internet of Things (“IoT”) – Includes data collected by biometric devices, driving monitors, virtual assistants, “smart” televisions, smart home devices including security and other appliances.

Corporate

- Identity & Data – This segment includes safeguarding access and data within the corporate network including file encryption, user identity and access controls.

- Network – This segment focuses on the various moats/walls companies put around their networks protecting them from unknown attackers.

- IoT – This segment focuses on security around manufacturing control and command including autonomous communication from sensor-laden production machines/devices.

Public

- Public Defence – This segment focuses on systems associated with physical defence as well as virtual defence (and offense too).

- Public Infrastructure & Services – citizen data, voting data, communications safeguarding/data, anti/counter-espionage, physical infrastructure command and control platforms.