FICO Decisions

WHITE PAPER

FICO® Enterprise Security Score: The Science of Cybersecurity Predictive Analytics

Managing Cyber Risk

1 Major, publicly disclosed data breaches highlight the increasing social and economic impact of cyber incidents. Without a new approach, these incidents will continue as organizations search for systematic and effective methods of assessing their security posture and quantifying the security risks throughout their supply chain.

2 Organizations are increasingly turning to cyber insurance coverage to offset their cyber risk exposure. While this growth has attracted new carriers and new classes of coverage into the market, the competitive pressures will force the adoption of quantitative methods in underwriting and pricing risk.

Predictive analytics provide the foresight to understand cybersecurity risk exposure.

Cybersecurity strategies often consist of "whack-a-mole" exercises focused on the perpetual detection and mitigation of vulnerabilities. As a result, organizations must re-think the ever-escalating costs associated with vulnerability management. After all, the daily flow of cybersecurity incidents and publicized data breaches, across all industries, calls into question the feasibility of achieving and maintaining a fully effective defense. The time is right to review the risk management and risk quantification methods applied in other disciplines to determine their applicability to cybersecurity. These proactive and systematic approaches may provide better quantification of the effectiveness of cybersecurity management practices.

The banking industry, as an example, bears similar risks in its management of credit card risk and has a long history of successfully applying predictive analytics and statistical methods to effectively identify, quantify and predict these risks. Forewarned is, after all, forearmed. If these predictive analytics could be used to harness the risk of data breaches, the damages (both financial and reputational) could be reduced or avoided by a data-driven organization. Similar large-scale data analysis and modeling techniques are commonly used to underwrite property and casualty insurance or assess credit or interest rate risk. In this paper we will explore the potential of forecasting cybersecurity risk with a detailed explanation of the underlying technologies and analytics.

The FICO® Enterprise Security Score uses a supervised, machine learning scoring technique based solely on empirical modeling, as opposed to expert judgment and the arbitrary assignments of weights to conditions.

Cybersecurity risk prediction is complementary to threat detection. The former facilitates a proactive approach to meaningful change in security practice, whereas the latter triggers tactical remediations.

FICO® Enterprise Security Score: predictive and empirical

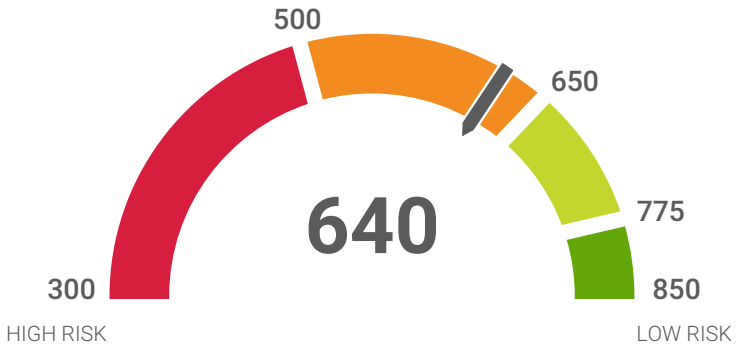
The current market is full of scores and ratings from companies that have an opinion about your security. These opinions are not based on empirical mathematical weightings between conditions, behaviors and cyber risk. In contrast, an empirical model is derived from data of past breaches and focuses on the factors that are demonstrably weighted to predict a given prediction target (i.e., a debilitating security incident). Empirical scores rely on derived mathematical equations between evidence and outcomes, rather than subjective opinion.

Producing an empirical model requires a deep understanding of the types of data required, methods of collecting historical data, and techniques that combine machine learning and cybersecurity domain expertise to create the predictive features used to derive meaningful and interpretable results. FICO's deep experience in developing predictive models and effective risk quantification tools provides us with a time-proven, market-accepted approach to tackling the problem of cyber risk quantification.

To understand what makes the FICO Enterprise Security Score different and reliable, it is necessary to clearly separate the detection of vulnerabilities and threat signatures from the prediction of forward-looking risk. This distinction is critical when comparing security ratings that rely on judgment to the Enterprise Security Score, which is a predictive model that is trained on historical data.

Ratings focused on the detection of threats will typically catalog binary yes/no conditions. The presence of certain conditions or vulnerabilities is then used to add or subtract an arbitrary number of points from a score or report card. This approach supports the "whack-a-mole" security strategy described earlier in this paper, but will not forecast future risk nor suggest more holistic strategies for long-term improvements. As key decisions such as insurance underwriting, establishing new vendor relationships or making key infrastructure investments require a forward-looking view of risk, a predictive analytics approach is appropriate to the business need.

The FICO Enterprise Security Score is an empirically derived, 3-digit predictive score that ranges from 300 to 850. The output can be broken down into four scoring bands, each representing the likelihood of a data breach over the ensuing 12-month period: high risk (300–500), medium risk (500–650), low risk (650–775) and very low risk (775–850).



The Data

Data richness is necessary for empirical analysis and predictive model development.

The key to empirical model development and predictive analytics is clean, relevant data. The dataset must contain sufficient depth and breadth in order to support the full analytical R&D lifecycle.

Measuring cybersecurity risk is a complex equation that involves evaluating a unique mix of technology, people, training, policies and procedures that are extant within an organization. An emerging consensus among practitioners is that security is not solely an IT issue. It is a process issue that involves the network team, the applications team, the products, services and support groups as well as procurement.

Internet Scale Measurements

The FICO® Enterprise Security Score utilizes a diverse set of inputs including the ongoing, Internet-scale collection of malicious activities and misconfigurations. Malicious activities encompass events at an organization that are related to potential botnet infections, such as spam propagation, hosting of phishing or malware sites, and scanning or attacks directed at other organizations. Misconfigurations focus on a wide variety of services and applications that organizations must enable in order to function effectively. These include various core servers and services such as web access or email and network infrastructure.

Inferred Behavior

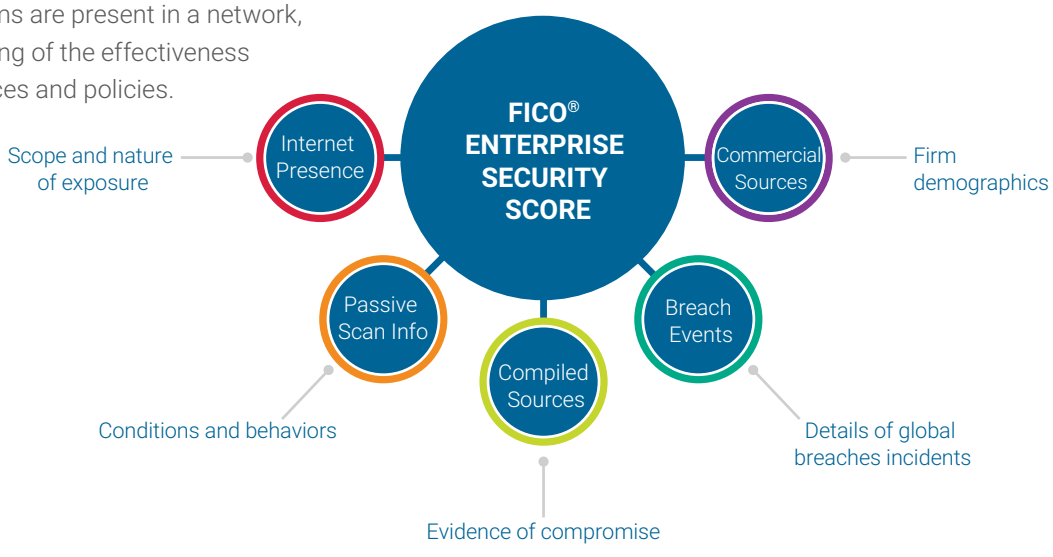
By continuously collecting information at scale, FICO is able to not only assess condition, but also organizational behaviors. By assessing how long issues or problems are present in a network, we can get an understanding of the effectiveness of an organization's practices and policies. Just as conditions can be correlated with risk, these observed behaviors or lack of urgency can be correlated with risk and provide even greater insight into the likelihood of future trouble.

Historical Depth

The data utilized by the FICO Enterprise Security Score reflects historical risk indicators from organizations around the globe. Machine learning is used to evaluate these indicators and understand their weightings, in combination, to provide a prediction of future breach events. These predictive models help forecast future events at other institutions.

Network Asset Discovery

One of the most challenging obstacles in developing a security score is accurately estimating the Internet footprint of a given organization. This includes the proper identification of network assets used by a specific enterprise, or subset of an enterprise. While publicly registered records provide a starting point, the FICO Enterprise Security Score allows clients to curate the assets being evaluated, in real-time.



The Model

Machine learning models automatically evaluate predictive features embedded in the data.

Model Development

The analytic models behind the FICO® Enterprise Security Score are developed using a supervised learning framework. This process uses FICO's continually updated collection of global Internet risk indicators, which provides a rich set of exemplars and contains the historical depth necessary to analyze the security practices of both breached and non-breached organizations. Using these outcomes as targets, predictive features are then extracted and machine learning is applied to determine the optimal mix of characteristics to predict future risk.

The output of the model, a 3-digit score that ranges from 300 to 850, represents the likelihood of an organization suffering a material data breach within the next 12 months. A higher score indicates lower risk, similar to a FICO® Score. The Enterprise Security Score is directly indicative of the absolute risk of a breach, rather than a judgmental score.

To aid in interpretation, the FICO Enterprise Security Score produces three reason codes with each score. The reason codes indicate the primary risk factors that drive the score, e.g., end-point long-term malicious activities, host population risk, and services and infrastructure attack surface, to name a few examples.

Model Performance

The FICO Enterprise Security Score model performance is evaluated using two widely accepted criteria: (1) the Area Under the Curve, or AUC, and (2) the dynamic range, or odds range, of the model output.

AUC is an indication of the accuracy of a model, i.e., how well the model is able to detect true positives while avoiding false positives. FICO's model has a very high AUC, and performs very well by this measurement. As FICO is continually improving its models, please feel free to ask your FICO representative about the current AUC performance.

The dynamic range of a model indicates how well the model is able to identify and separate goods (organizations without a disclosed cyber breach event) from bads (organizations with a publicly disclosed cyber breach event). At the time of publication of this paper, FICO's models have 4x the dynamic range of the competitors' published results. As FICO is continually improving its models, please feel free to ask your FICO representative about the latest dynamic range performance.

Illustrative example of score separation. Not reflective of FICO® Enterprise Security Score actual performance.

Odds vs. Probability

The FICO® Enterprise Security Score rank-orders organizations according to their relative likelihood of suffering a material breach event. For example, even organizations receiving the best score (i.e., 850) are not impervious to internal and external threats and subsequent data breach. However, their odds of suffering a breach are significantly lower than organizations receiving lower scores. This is quite different, and more useful, than attempting to forecast the probability of a data breach (i.e., a 40% chance). The FICO Enterprise Security Score supports proper contingency planning and provides risk management professionals with the details needed to evaluate and monitor security performance over time.

Conclusion

Security scoring is a hot topic, and rightfully so. When evaluating ways to integrate these scores into your cybersecurity strategy, be sure to look for an empirical approach to model development. The FICO Enterprise Security Score is the most accurate, predictive security score on the market.

To learn more, visit securityscore.fico.com.

FICO

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com

4417WP_EN 06/17 PDF