Carrier Management

Cyber FICO Ratings Could Benefit Insurance Underwriting in Multiple Ways

Written by Michelle Reed, Shawn Hanson and Diana Schaffner

Nearly 30 years ago the Fair Isaac Corporation ("FICO") first introduced its metric for measuring creditworthiness. Since then, the FICO Score has become a default metric used by countless market participants to facilitate arms-length transactions. It is a score that, while not without problems, is generally understandable and easily accessible.

FICO and other entities are now promoting new methods of rating companies' cyber risk and resiliency with the same goals of promoting informed decision-making. The growing importance of such ratings was recently recognized by the U.S. Chamber of Commerce, which published "Principles for Fair and Accurate Security Ratings" in June 2017. This article briefly discusses the growing role of security ratings in driving business strategy and the need for more uniform standards among ratings companies.

External Scores

The goal of a security rating is to assess a company's general degree of cyber risk and how prepared the company is to withstand cyber attacks or cyber incidents. Security ratings are an externally-focused means of measuring a company's cyber resiliency. In this way, they are akin to the FICO Score inasmuch as they rely on external data to provide a risk profile without need for input or cooperation from the rated company.

Every company with a digital presence has an Internet footprint, including devices and data belonging to the company that are accessible (intentionally or not) from the Internet. Security ratings analyze this outward-facing footprint to assess the company's cyber weaknesses and levels of risk. The main benefit to this method of assessment is that it can be determined

Originally Published Feb 6, 2018 (Redistributed with Permission)

externally. The methods of measurement and comparison between companies also can be standardized to provide for meaningful comparisons within and across industries.

These ratings are being used, and will be used with increasing frequency, to determine whether to underwrite cyber insurance policies, whether to hire certain vendors, and whether to make certain business acquisitions. A number of startups and new companies are entering the field, along with established players like FICO, to provide security ratings.

Two Key Benefits

There are two key areas in which security ratings are likely to have the greatest overall market benefit:

- Promoting informed underwriting with regard to cyber liability policies, including enabling better informed pricing for and thereby potentially increasing access of small and medium-sized businesses ("SMBs") to cyber insurance.
- Helping companies select strong vendors and decrease risks posed to their systems by third parties.

Benefits in Promoting Informed Underwriting – Security ratings are developing into an important resource for insurers with regard to underwriting decisions on cyber liability policies. The greatest challenge facing the cyber insurance industry, aside from the continuing rise in the number of cyber incidents, is the relative lack of reliable information to feed into the underwriting process (given the relative youth of the cyber insurance market). The nature of incidents and the scale of risks are more difficult to map as compared to the damage arising from a fire, flood, or employee theft. Currently, cyber insurers often rely on questionnaires and feedback from the company seeking insurance to provide a view on the company's existing cyber resiliency. An independent rating can help identify risks and weakness the company itself may not understand, or could otherwise mask. The use of objective measures and standardized systems for comparing companies' cyber ratings may also be a more efficient means of obtaining certain information.

Smart security ratings may have a particular effect with regard to underwriting cyber liability insurance for SMBs. Currently, only a small percentage of SMBs have cyber insurance. The unmet need is so great the U.S. House of Representatives Small Business Committee held a hearing in July on ways to promote additional coverage. SMB-focused cyber ratings, that incorporate the U.S. Chamber of Commerce's Principles, could help insurance companies determine which SMBs to insure and to fairly price policies. Using data-driven risk scores can help carriers reduce risk and properly price policies for the growing, unmet need among SMBs.

Benefits in Helping Companies Select Vendors – Robust and fair cybersecurity ratings also benefit companies during the vendor selection process. Currently, as with cyber insurance, companies rely on vendor question-

naires, site visits, etc. to try and gauge a potential vendor's cyber risks. A company's systems are only as strong as its weakest vendor when it comes to cybersecurity. Today, companies are often in the dark about the actual strength of a potential vendor's cybersecurity, privacy, and data protection systems. Depending on the size and bargaining strength of the vendor, some vendor contracts are written in a manner that severely limits a company's ability to recover from a vendor after a cyber-incident. This leaves companies on the hook for costs related to, among other things, consumer notifications, civil litigation, or regulatory investigations. Security ratings provide a simple and accessible way to evaluate the cyber posed by a vendor before signing a vendor agreement.

Potential Risks from Use of Security Ratings

Use of security ratings does not come without risks. Evaluation methods intended to provide security ratings for companies generally, likely will not take into account the variation in security standards typically applied among companies of different sizes or industry-specific differences. Cyber threats also change regularly and prescriptive standards are often out of date before they are published. Use of security ratings could also lead companies to secure to the score, rather than performing a risk assessment and prioritizing cybersecurity actions based on the most important needs of the company itself.

The use of security ratings may give disproportionate power to those establishing the criteria used to assess the scores. Ratings companies often claim that their methodologies and standards of comparison are proprietary information. What factors go into evaluations and the relative weight of various factors remain opaque. Companies that are rated have complained of a general lack of transparency in the process, as well as an inability to challenge the results.

In June 2017, the U.S. Chamber of Commerce issued its "Principles for Fair and Accurate Security Ratings" with the goal of addressing some of these concerns. These Principles were immediately embraced by over two dozen organizations, including major financial services institutions and some ratings companies. There are six key principles:

- Transparency (into ratings methodologies and the data used for particular companies);
- Dispute, correction and appeal (rated companies should be able to dispute scores, provide corrected data, and engage in a dispute resolution process);
- Accuracy and validation (ratings companies should use empirical methods and provide validation for their ratings);
- Model governance (ratings companies should notify rated companies prior to changing their methods of measurement);
- Independence (commercial relationships should not affect ratings and companies should be able to access their ratings);
- Confidentiality (information shared as part of the ratings process should be protected and ratings should not be publicized).

If implemented, these Principles may go far in promoting fair and accurate security ratings.

Why Now

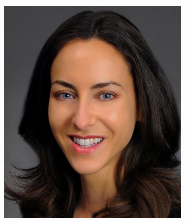
In the post-Equifax world, companies are increasingly accepting that strong cybersecurity means focusing on managing, rather than eliminating, cyber risk. This is particularly true as more and more companies partner with cloud service providers or rely upon third-party vendors to provide key services. In this increasingly complex risk environment, cybersecurity ratings carried out by external, independent ratings companies play a key role by supporting informed decision-making without the need for cooperation from the rated company. CM

Michelle Reed, Akin Gump

Michelle Reed is a partner and co-leader of Akin Gump's cybersecurity, privacy and data protection practice. A Certified Information Privacy Professional (CIPP/US, International Association of Privacy Professionals), she counsels corporations in data breach investigations and notifications, SEC cybersecurity compliance and regulatory issues, privacy and data protection compliance and cloud computing advice.

Shawn Hanson, Akin Gump

Shawn Hanson is a partner in Akin Gump's litigation practice. He advises insurance companies on a wide of range of regulatory issues, including compliance with existing and evolving regulations and analysis of state and federal-level regulatory frameworks, with a particular focus on the intersection of insurance and technology.



Diana Schaffner, Akin Gump

Diana Schaffner is counsel in Akin Gump's litigation practice and a member of the firm's cybersecurity, privacy and data protection practice. She advises on related compliance matters and litigation.