Information Security Risk and the Need for Quantitative Ratings

M. Eric Johnson | September 2013

ABOUT THE AUTHOR

M. Eric Johnson is the Ralph Owen Dean of Vanderbilt University's Owen Graduate School of Management. His teaching and research focus on the impact of information technology on the extended enterprise. He has authored patents on interface design and has testified before the U.S. Congress on information security. [1]

Linkedin: www.linkedin.com/pub/m-eric-johnson/3/917/43

INTRODUCTION

Risk is part of every business decision. Many risks can be quantified, priced, and thus effectively managed through financial instruments and portfolio management. However, information security risk, particularly the risk posed by a business partner, has proven to be a more significant challenge.

This paper examines the need for objective security risk ratings. This is done via a comparison with the credit rating industry, one that has been prosperous for almost a century. The credit rating industry was born from the need to provide investors information and objective analyses on investment opportunities. By bringing transparency to the investment process and reducing the time and cost of analyzing opportunities, credit ratings played a significant role in the development of the securities market.

*This paper is based, in part, on a previous paper by Eric Johnson and Igor Macura entitled "Information Risk and the Evolution of the Security Rating Industry," published in March 2009.

[1] http://www.owen.vanderbilt.edu/vanderbilt/faculty-and-research/faculty-directory/faculty-profile.cfm?id=273

The Corporate Credit Rating Industry

A corporate credit rating is an opinion of the relative credit quality of an organization's obligations (such as a bond) or of an issuer's general creditworthiness. The specialized companies that issue the ratings are commonly referred to as credit rating agencies (CRAs). CRAs act as an intermediary between the issuer and investor and provide information asymmetry about the riskiness of investment opportunities. The credit rating process involves developing and using methodologies to analyze and predict the performance of financial products and underlying assets. In doing so, CRAs rely on advances in the theory of finance, as well as empirical analysis using available historical data.

EVOLUTION

The credit rating industry was established in 1909, when John Moody published a book titled Moody's Analyses of Railroad Investments. The Analyses contained data and ratings for more than 250 railroad bonds. The volume proved a success - the whole circulation was sold within three months of the publication date. The ratings coverage then expanded to industrial companies, utilities, and municipalities. By 1924, Moody's Investors Service issued ratings for nearly the entire US bond market.

In 1931, the Office of the Comptroller of the Currency (OCC), the federal bank regulator, required banks to use current market prices for all the bonds on their balance sheet rated below "investment grade". This was the first case of a formal regulatory endorsement of debt ratings. In 1936, the OCC went further and restricted banks from buying bonds below "investment grade". In the following decades, dozens of regulations included references to ratings, increasing the influence of CRAs. Today there are three main CRAs - S&P, Moody's, and Fitch - whose combined market share is 95%.

The rating process is initiated and paid for by a securities issuer. For a first-time rating, the process begins with an introductory meeting where issues such as the industry environment, operating results, management structure, corporate strategy, debt structure and financial position of the entity bring rated are discussed. This is done with a mix of publicly available and nonpublic data on the Company. After further discussions, the lead analyst presents the conclusions to the CRA's rating committee, and the committee votes on the rating. Once the rating committee has made its decision, the issuer is informed of the rating and rationale and may have an opportunity to provide additional information before the rating is published. For a public rating, the new rating is distributed by press release simultaneously to the major financial media worldwide. Once published, ratings are continuously monitored and updated through dialogues and regular meetings.

REASONS FOR SUCCESS

A testament to its value, a credit rating has become a precondition for a debt offering in virtually every country. As CRAs established a reputation as a reliable and widely used source of information about the riskiness of securities, the number of market participants and investment opportunities grew, thus creating stronger capital markets. Borrowers and lenders, who may have otherwise been shut out, now participate in the market.

The success of credit ratings can be broadly attributed to the following four characteristics:

- **Simplicity**: Everyone understands the ratings scale. Even for people who are new to investing, the rating scales used by the different CRAs are easily comprehensible;
- **Scope**: All public credit ratings are published and available on CRAs' websites. Ratings for private placements of securities may be nonpublic. Any Company / security issue that fulfills the CRA's set of criteria, can seek to be rated;
- **Comparability**: The above two factors enable quick and effective comparisons across securities;
- **Accuracy**: To increase transparency, information should be accurate, and be seen as accurate by investors. For this, credibility of the CRA is crucial. On the other hand, inaccuracy in ratings and the use of such ratings in the calculation of capital requirements can lead to systemic risk with potentially severe negative consequences. This is an ongoing area of debate and analysis.

CHALLENGES

Although the credit rating industry has generally been viewed as a successful one that has played an important role in global economic development, it does suffer from a few problems that hinder the last success criteria discussed above – accuracy. These problems have been widely discussed, particularly since the 2008-2009 financial crisis, and revolve around the inherent conflict of interest in the issuer-pay model. Large issuers contribute a significant portion of a CRA's revenue and thus CRA's have a natural desire to gain their business, possibly by issuing higher than justified ratings.

An analysis of 39,000 quarterly bank ratings issued by S&P, Moody's and Fitch over the period 1990 to 2011 conducted by Hau, Langfield and Marqués-Ibañez (2012) suggests that "rating agencies assign more positive ratings to large banks and to those institutions more likely to provide the rating agency with additional securities rating business (as indicated by private structured credit origination activity)." [2] In February 2013, the United States Department of Justice filed a civil lawsuit against S&P alleging that S&P issued inflated ratings that misrepresented the true credit risk of structured financial products in a scheme to defraud investors.

Related problems include ratings shopping, wherein CRAs complete by inflating ratings, and ability of issuers, through their arrangers, to construct structured products just to meet certain rating levels.[3] In addition, some empirical literature finds that ratings changes generally lag the market.[4]

Information Security Risk

The advances in information and communication technology over the last decade have significantly broadened the scope of interaction among organizations and individuals. While this development means new business opportunities for companies, such as process acceleration, outsourcing, and telecommuting, it also brings with it increased information security risks. These risks manifest themselves through hacker attacks, spyware proliferation, various types of data theft, virus infections, etc. Verizon, in its 2013 Data Breach Investigations Report (DBIR), reported 47,000+ security incidents and at least 44 million compromised records. [5] According to the Ponemon Institute, the average cost of a data breach in the U.S. was $5.4 million in 2012. [6]

[2] Working Paper "Bank Ratings – What Determines Their Quality" by Harald Hau, Sam Langfield and David Marques-Ibanez: <http://www.ecb.int/pub/pdf/scpwps/ecbwp1484.pdf>

[3] Economic Analysis of credit rating agency business models and ratings by Fennell, Medvedev 2011: <http://www.fsa.gov.uk/pubs/occpapers/op41.pdf>

[4] Financial Economists Roundtable 2008 - <http://fic.wharton.upenn.edu/fic/policy%20page/FER12%201%2008rev.pdf>

[5] 2013 Data Breach Investigations Report: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf>

[6] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, March 2013

A growing area within security risk is partner security risk. Companies share sensitive data with business partners globally and have little visibility into the security posture of those partners. In a 2013 Ponemon Institute survey of companies that outsourced data to a third party, 65% of participants said their organization had a breach involving the loss or theft of their organization's information via a business partner. [7]

NEED FOR INFORMATION SECURITY RATINGS

Just as the financial industry needed independent credit ratings to increase transparency and decrease information asymmetry, businesses require information security ratings to understand the risk of sharing sensitive data with business partners. As in the case of financial risk prior to 1909, there is little publicly available information today about security risk. There are two key differences between financial risk and security risk that make security ratings all the more necessary:

- Financial risk can be mitigated through diversification. Investors can diversify their security holdings. Businesses can spread financial risk across multiple products, customer segments, and geographies. If one product does not meet revenue expectations, the shortfall can be made up by other products. In contrast, security risk is difficult to mitigate through diversification. For example, the risk of sharing employee data with a payroll processor cannot be mitigated by using two processors. Such a practice could limit the scale of a breach since neither processor has all the data, but it actually increases the chance of a breach because there are now two partners who could be hacked.

- If financial risk is properly diversified, the downside is known and limited. In the case of cyber risk, the impact – financial and reputational – is potentially unlimited. Moreover, the losses could be much larger than the value of the service provided by the vendor. If they have the appropriate coverage, cyber insurance holders can recover the financial cost of a breach. However, intangibles, such as loss of customer trust and reputation, cannot be quantified or easily recovered.

Many tools are available today for companies to manage their internal security risk. Some work, others do not. Much depends on the skills and resources available to manage those tools. Successfully deployed firewalls, intrusion detection and prevention systems, vulnerability assessments, and security information management tools can provide a great deal of visibility into a company's own security posture. However, in spite of the proliferation in the number and type of security solutions over the past two decades, organizations do not have a good understanding of their risk exposure. The Verizon's 2013 DBIR reports that 66% of breaches took over one month to discover (compared to 56% in 2012). The report further mentions that 69% of breaches were discovered by external parties (including customers) and not by the organization that was breached. [8]

Organizations have far fewer tools to assess the security posture of partners with which they share sensitive business data. The most widely used tool is an information security assessment prior to onboarding a new partner. These assessments are questionnaire based, and ask about the partners' policies and procedures. The answers are subjective as they are based on the opinion of the responder. They are also based on information available at that point in time, and thus reflect a static opinion. Large organizations may reassess their critical vendors on an annual basis. However, many organizations do not have the resources to do even a preliminary security assessment when first onboarding a new partner. At best, organizations have a static and subjective view on their partners' policies and procedures. At worst, they are totally blind to partner security risk.

[7] Securing Outsourced Customer Data, Ponemon Institute, February 2013

[8] 2013 Data Breach Investigations Report: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf>

Companies that are breached are often compliant with applicable regulations, such as Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS) and the Health Information Portability and Accountability Act (HIPAA). In fact, recent research indicates that there is little association between compliance and actual breach performance in firms with active security programs. [9] Compliance with these regulations means that companies have the appropriate policies and procedures in place, not that they are properly implemented or updated based on the changing threat landscape.

The need for evidence-based, timely security ratings generated by an external entity is clear. A ratings system, if properly created and implemented, will bring transparency to the murky science of security risk management. Just as credit ratings enable investors to make risk based investment decisions, security ratings could enable organizations to make risk based decisions on their internal security investments and on their partner ecosystem.

CRITERIA FOR SUCCESS

Many of the learnings from the credit ratings industry can be applied to security ratings. The same four factors that were key to the success of credit ratings will also be important to the market adoption of security ratings. Each factor is discussed below with security ratings in mind.

- **Simplicity**: Like credit rating scales, security rating scales must be well defined, easy to comprehend, and applied uniformly to all entities being rated.
- **Scope**: Ratings must be available for a large number of companies, in all industries and in all regions of the world. The wide range of ratings will allow companies to compare themselves and their business partners with others in the same industry or geography.
- **Comparability**: The security rating of any company should be comparable with that of any other company.
- **Accuracy**: While one hundred percent accuracy cannot be guaranteed, rating trends and relative ratings should be viewed as directionally accurate, objective and timely. [10] If security ratings are not indicative of the company's current security posture, they will not be widely adopted.
    - Like credit ratings, security ratings should be data driven and based on outcomes rather than policy. For example, credit ratings are based on the financial standing of a company (cash on hand, revenues, etc.) rather than on the financial policies in place. Similarly, security ratings should be generated on the actual security posture of a company rather than on its security policies.
    - To avoid the conflict of interest created by CRAs business model of having the issuer paying for the rating, the security ratings industry should seek an alternative business model.

In 2008, Moody's launched a vendor security rating service. Its business model required the entity being rated to pay for the service, thus bringing into question the accuracy of the ratings. In addition, the ratings were questionnaire based and required significant effort on the part of the company being rated. Thus, few companies subscribed to the service. It is important for any new security ratings scheme to employ an unbiased, evidence-based model and offer a service that is more automated and affordable.

[9] Kwon, Juhee and M. Eric Johnson (2013), "Healthcare Security Strategies for Information Security and Regulatory Compliance," forthcoming in Journal of Management Information Systems.

[10] Crowther, Kenneth G., Yacov Y. Haimes, M. Eric Johnson (2010), "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," Journal of Homeland Security and Emergency Management, Vol. 7, No. 1, 1-18.

BENEFITS

The benefits of an external, objective security rating system are plenty. There are significant opportunities to achieve reduction in costs by having a few reputed services gather and process the data required to develop ratings. Economies of scale ensure largest possible coverage of organizations being rated and widespread dissemination of analysis.

Well understood ratings will allow companies to make risk based decisions – do they need additional investment in security products or services? In which areas? Should they trust their sensitive information with a certain business partner? How should they negotiate with a vendor related to securing data? Ratings could also be used to assess investments, acquisition opportunities, and cyber insurance applicants.

Conclusion

The market need for an information security rating is clear. The benefits show that objective, data driven ratings would be superior to current solutions, which are costly and of limited effectiveness. Whether the information security rating industry will be established is not the question; but rather how will ratings be generated in an objective and cost effective fashion? Will they reflect current risk? And how quickly will the market adopt these ratings?