GARCH-based IT Risk Assessment and Mean-Variance-based Risk Mitigation Framework

TREO Talk Paper

Baidyanath Biswas
Indian Institute of Management Lucknow
fpm15005@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow
arunabha@iiml.ac.in

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

Abstract

Security vulnerabilities in software products are exploited by attackers causing breaches and cyber-attacks. While there were only 890 known vulnerabilities in 1999, their count increased to a total of 79440 in 2016. The National Vulnerability Database (NVD) reports 4800, 3950 and 3500 vulnerabilities respectively for top software vendors: Microsoft, Oracle, and Apple. Often publicly disclosed vulnerabilities instigate attacks in organizations including market-based disclosures. Security vulnerabilities exploits may even originate from the same or different products of a software publisher. A series of vulnerabilities disclosed in July 2016 for Cisco network devices could create a DoS attack. Exploits followed, and more vulnerabilities were disclosed till September. Above incident demonstrates clustering effect in vulnerability growth similar to autoregressive conditional heteroscedasticity for financial assets.

We intend to answer the following questions through this study: (i) How do vulnerability exposures in software change with time? (ii) Are we capable of accurately predicting software risk for the future in terms of volatility growth? (iii) How do user firms diversify their software investments to optimize the risk exposure? (iv) Based on the threshold risk profile and IT budget, what diversification strategies can firms possibly adopt? Next, we also aim to analyze the current literature on vulnerability discovery with the following methodological lenses that use actual disclosure data: vulnerability discovery models (VDM), and econometric models. While econometric models perform better estimation and forecasting, extant literature does not explore them in detail. Furthermore, they employ linear prediction techniques but ignore heavy-tails and non-normality. Next, our efficient software portfolio analysis is based on a mean-variance approach where the risk-averse user aims for lower variance and higher returns.

We draw the theoretical foundation for our framework from corporate IT governance. Business investments in information technology directly impact the effectiveness of governance. Firms apply IT in multiple ways to frame key firm-level decisions. Often, the IT investment decisions are largely dependent on the distribution of the respective corporate portfolio structures and successful synchronization with business objectives. Also, strategic information system planning (SISP) needs alignment of business with IS/IT, and security investments are no exception. Due to the positive network effects, organizations ignore software diversity, leading to monopolization of a particular software platform. Such a scenario can magnify the security vulnerabilities in the ecosystem of the enterprise network under attack.

The CVE entries for top software publishers from NVD serve as our dataset of analysis. For a firm with software purchase, we simulate the benefits and correlated risk with multiple combinations. We minimize the correlated risk and maximize expected benefits by proposing efficient software portfolios. Also, our framework takes into account the change in portfolio over time and align it with their business goals for effective IT governance and IS/IT investments. CTOs and CISOs can monitor the state of their software and networks and reassign future investments. It will assist firms to assess IT risk, manage vulnerabilities, and plan IT security investments, mitigation strategies. In future, we intend to combine vulnerability data from multiple sources – both private and public, to enrich our study and discover further stimulating results.