# Vendor Risk Rating Correlation to Data Breach Event Frequency

Predicting third-party breach event frequency with cybersecurity ratings and insights

# Introduction

Third-party risk management teams are charged with protecting the organization's assets across hundreds and sometimes thousands of organizations. Which vendors represent the greatest risk and what should I do about it? RiskRecon's ratings and insights help answer these questions, making it easy to understand and act on your third-party cybersecurity risks.

RiskRecon's cybersecurity rating model strongly predicts the breach event frequency to expect from companies in different rating tiers. Based on analysis of the RiskRecon ratings and breach event data of nearly 46,000 companies, companies in the "F" rating tier have a four times higher breach event frequency than do companies in the "A" rating tier.

RiskRecon did not set out to build a model to predict data breach events. Rather, the rating model is designed to measure the quality of the organization's cybersecurity risk management as observed in the reality of "known good" and "known poor" risk management performance. For example, banks are known to manage risk better than universities.

Though RiskRecon did not intentionally build its rating model to predict breach events, the model does strongly predict the frequency that breach events will occur. Go figure, companies that measurably demonstrate good cybersecurity risk management practices have much lower rates of breach events than those that do not. Let's dive in and talk about the methodology, the results, and why it matters to you.

# The Methodology

RiskRecon's study of ratings and breach event frequency, conducted in December 2020, was based on analysis of 45,641 companies for which RiskRecon maintains analyst-trained assessment profiles. These companies span all industries – retail, financial, healthcare, public administration, education, manufacturing, professional services, and so forth. For each of these companies, RiskRecon had identified 5,464 data breach events.

For each company, RiskRecon removed the impact of any breach events on the company's rating. This left company ratings to only reflect the quality of their cybersecurity risk management. RiskRecon then divided companies according into rating bands, along the A – F rating scale, and calculated the breach event frequency per band.

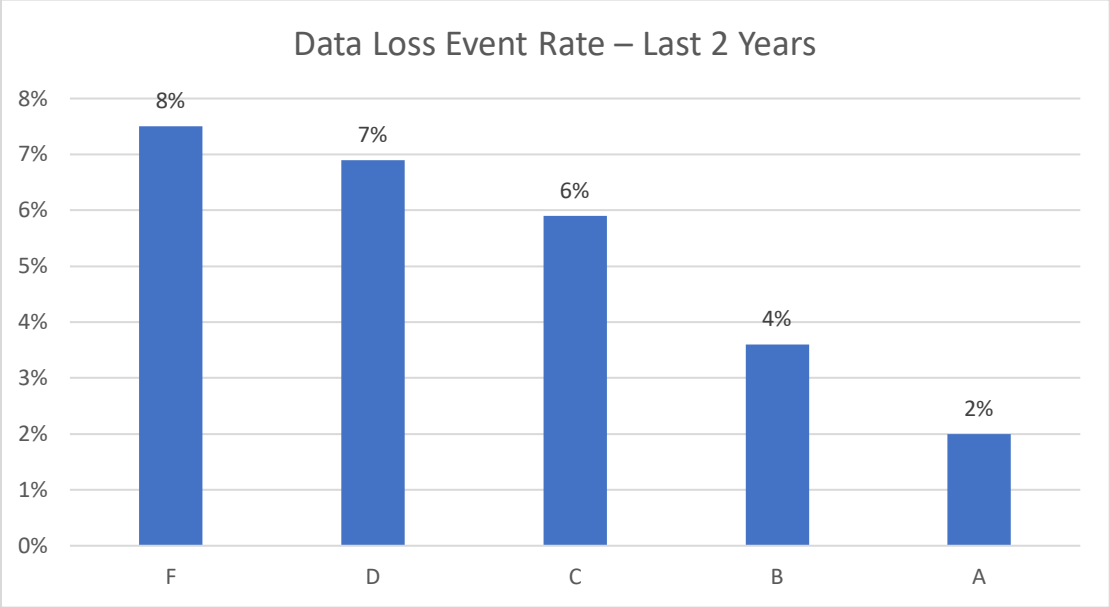
# The Results

RiskRecon rates cybersecurity risk management performance on an A – F rating scale, with F being the lowest rating. For each rating tier, RiskRecon calculated the breach event frequency across three spans of time: events occurring in the last two years, in the last five years, and breach events occurring across all time.

<u>Data Loss Events per Company – Last Two Years</u>

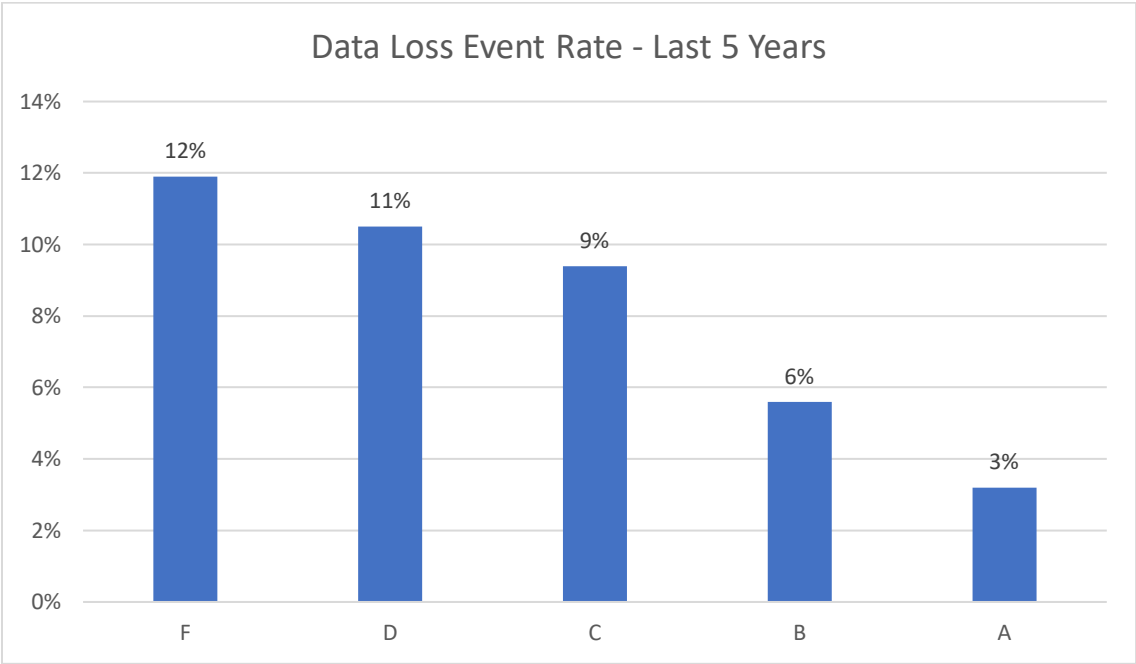
When factoring only data loss events occurring in the last two years, companies rated as "A" had two data breach events per 100 companies, while companies rated as "F" had eight breach events per 100

companies. F-rated companies have a 4x higher rate of breach events compared with A-rated companies.



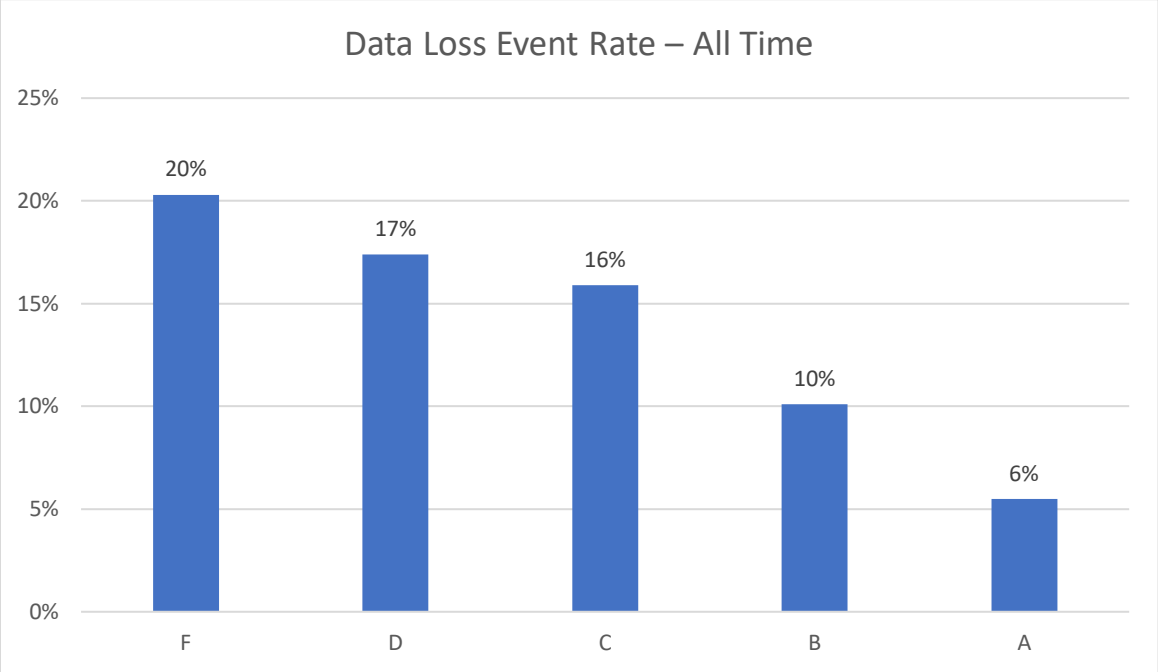

Data Loss Events per Company – Last Five Years

When factoring only data loss events occurring in the last five years, companies rated as "A" had three data breach events per 100 companies, while companies rated as "F" had twelve breach events per 100 companies. Again, F-rated companies have a 4x higher rate of breach events compared with A-rated companies.



Data Loss Events per Company – All Time

When factoring all data loss events occurring across all time, companies rated as “A” had six data breach events per 100 companies, while companies rated as “F” had twenty breach events per 100 companies. F-rated companies have a 3.3x higher rate of breach events compared with A-rated companies.




## Why it Matters to You

You are charged with protecting your organization’s risk interests across a growing number of vendors and partners, commonly numbering into the hundreds and, sometimes in some cases, into the thousands. You have limited resources to manage your third-party risks. RiskRecon’s cybersecurity ratings and insights make it easier for you to understand and act on your risks. The companies with the lowest rating have the highest breach event frequency; prioritize your attention towards those companies. And when you do engage, RiskRecon’s objective insights help direct you towards the material issues that require remediation and the root cause security program gaps to address. Once you have completed your engagement, RiskRecon automatically monitors vendor progress, enabling you to hold your vendors accountable to protecting your risk interests well.

For additional information, please contact:

CyVent
PLAN. PROTECT. PRE-EMPT

1395 Brickell Av. #800
Miami, FL 33129
+1 305 299 1188