RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: SDS-R03

Applying Statistical Analysis to Third-Party Risk Assessment

Bill O’Connell

VP Chief Business Security Officer
ADP

The Premise

- It’s long been the case that vendors represent one of the greatest data protection risks for virtually every organization.
- The General Data Protection Regulation (GDPR) and other regulations have only increased that anxiety.
- With limited resources, and new innovations, how can we apply statistical analysis to our third parties to more efficiently and effectively manage these risks?

Third Parties and Risk

- Enterprises might ask:
  - Who has my data?
  - How are they using it?
  - Do I consent to that use?

- Regulators may ask
  - How did you get that data?
  - How are you using it?
  - Did the data subject consent to that use?

What Can You Do About the Risk?

- Understanding and managing the risks to your business by employing the use of any External Entities (Suppliers, Partners, Vendors, Third Parties, etc)

~~Ignore~~

What are your goals?

? Make regulators happy

? Keep my Job

? Manage Risk for my company

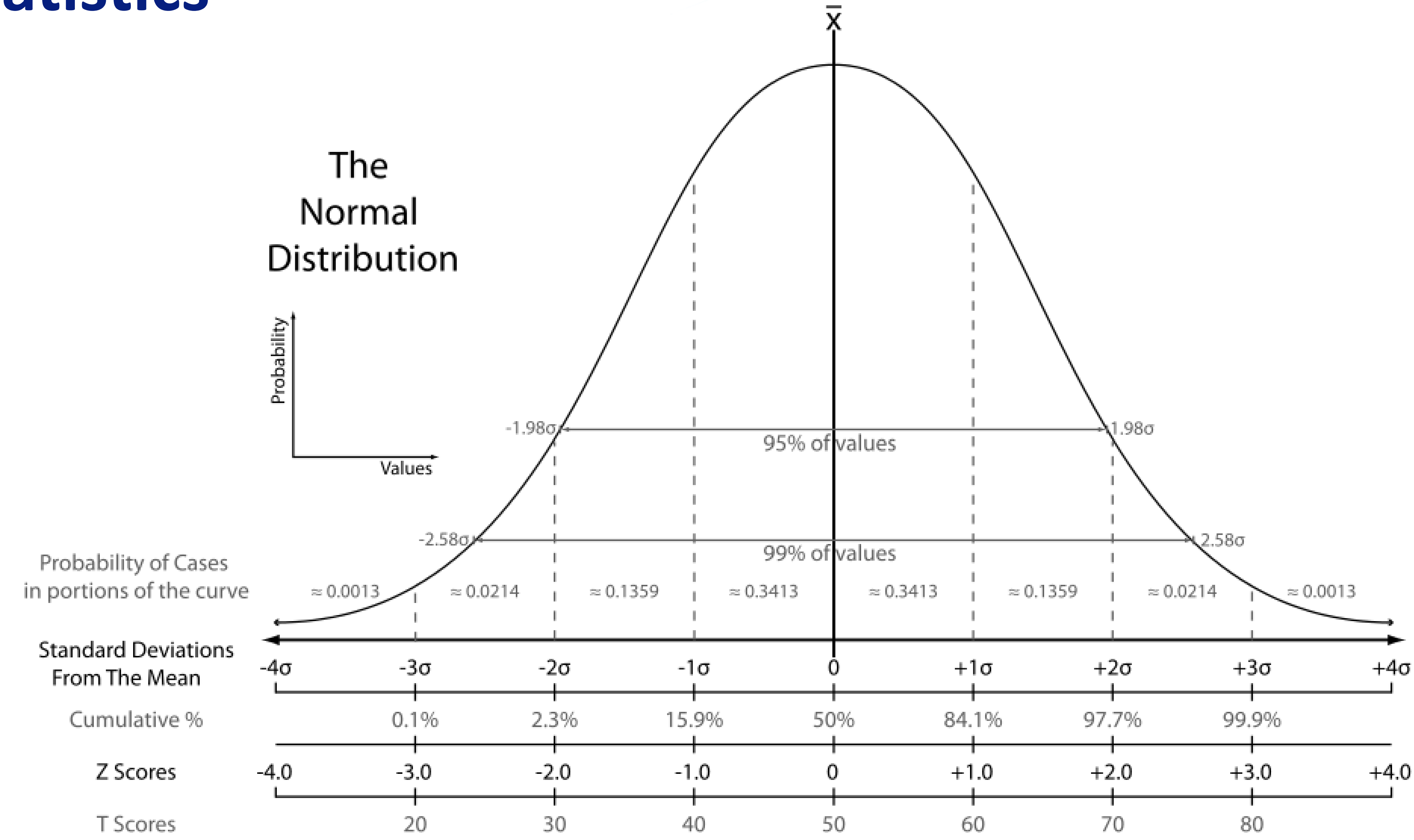
Is There A Better Way?

- Risk Based Approach
- A Common Assessment
- Taking actions that add value (ROI)

What Can You Do?

- Figure out what’s important
- Rank them all
- Group them into buckets
- Approach the buckets differently
- (Tell Mgmt you’re doing this)

Statistics


x̄
The Normal Distribution
Probability
Values
-1.98σ
1.98σ
95% of values
-2.58σ
2.58σ
99% of values
Probability of Cases in portions of the curve
≈ 0.0013
≈ 0.0214
≈ 0.1359
≈ 0.3413
≈ 0.3413
≈ 0.1359
≈ 0.0214
≈ 0.0013
Standard Deviations From The Mean
-4σ
-3σ
-2σ
-1σ
0
+1σ
+2σ
+3σ
+4σ
Cumulative %
0.1%
2.3%
15.9%
50%
84.1%
97.7%
99.9%
Z Scores
-4.0
-3.0
-2.0
-1.0
0
+1.0
+2.0
+3.0
+4.0
T Scores
20
30
40
50
60
70
80

Return On Investment

- Define your metrics
- How significant are the vendors you’re using?
- How much do they mean to your business?
- What would happen if they had a breach, or went out of business?
- How does any assessment you do help support your business?

Statistics: 1- Start with a Perfect World

- What are all of the variables that you could use to differentiate your vendors?
  - Demographics (Industry, Size, Location)
  - History (Years in business,
  - Functions (what will they be doing, how do they do it)
  - Effectiveness (Regulated?, Certifications?...)

Statistics 2: Adjust For The Real World

- Do you have all of this data?

- How easily accessible is it?

Statistics 3 – Do the Analysis

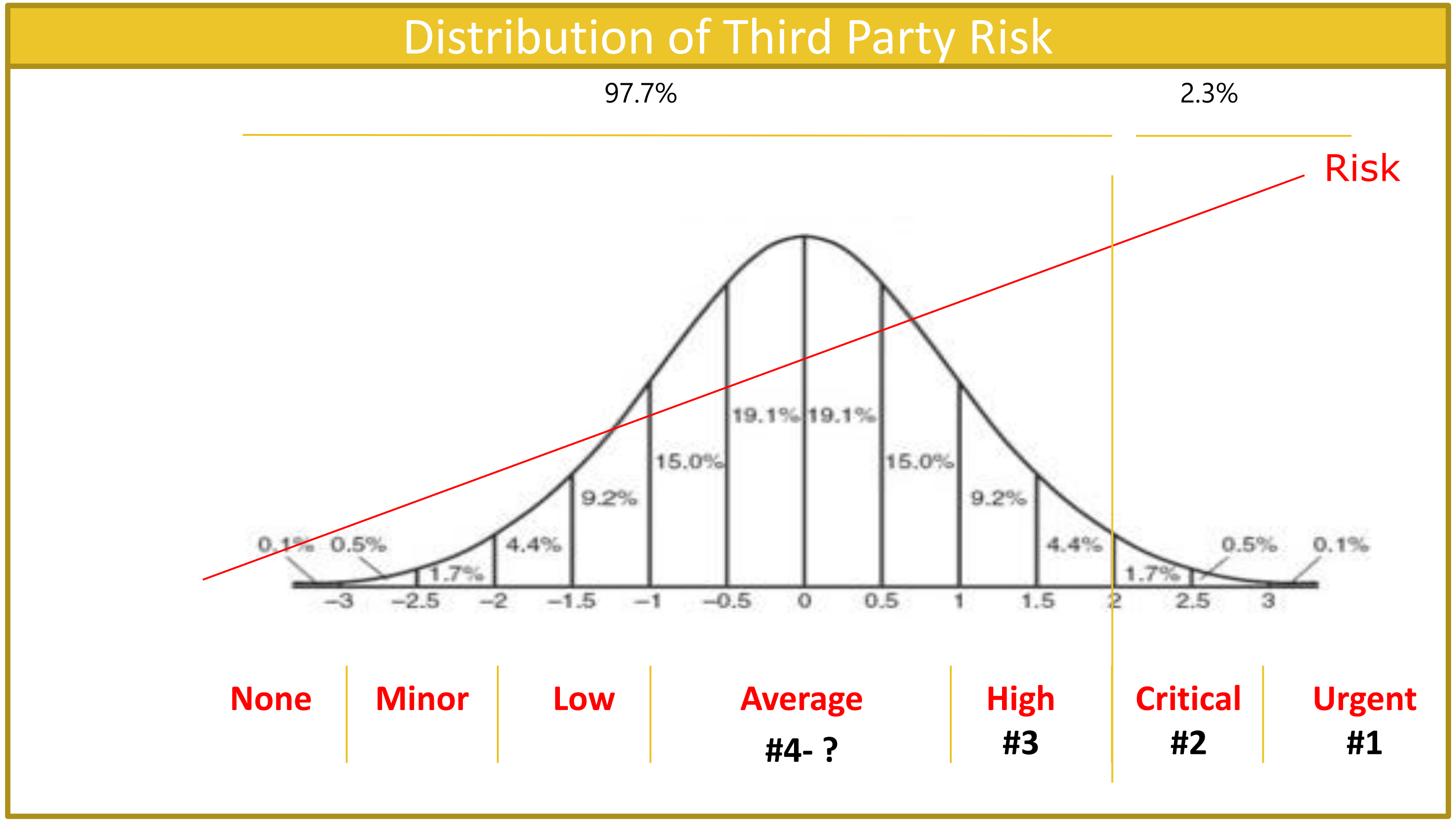
- Regression Analysis of variables (What data is more impactful than others?)

- Example
  - Does Location make any difference on risk?
  - How much more significant a difference on risk is Being Regulated

Statistics: 4- Compare The Past To The Future

- Collect the same data from current and future third parties
- Apply the past results to the future

What Will You End Up With?



Distribution of Third Party Risk

97.7%

2.3%

Risk

None

Minor

Low

Average #4- ?

High #3

Critical #2

Urgent #1

Action 1: Review Contracts

- Partner with groups that sign contracts: Procurement, Finance, Facilities, Marketing, etc.

- Get appropriate insight into the contracts

- Create a Standard Process for them to Alert and/or Involve your team

Action 2: Develop Standardized Contract Language

- Review the most common aspects that come up and develop standard contract language
  - A. Always Use
  - B. Be selective with this
  - C. Carefully use this
  - D. Don’t Ever

Action 3: Inventory Your Third Parties

- Partner with groups that have insight into your third parties: Legal, Procurement, Finance, Facilities, IT, etc. Quick Trick: Check your Accounts Payable!
- Check for Free applications (ask you IT Management team)!
- Remember the first rule of risk is understand the full landscape of what it is that you have to protect
- Develop an appropriate tracking system to identify them and manage their risk

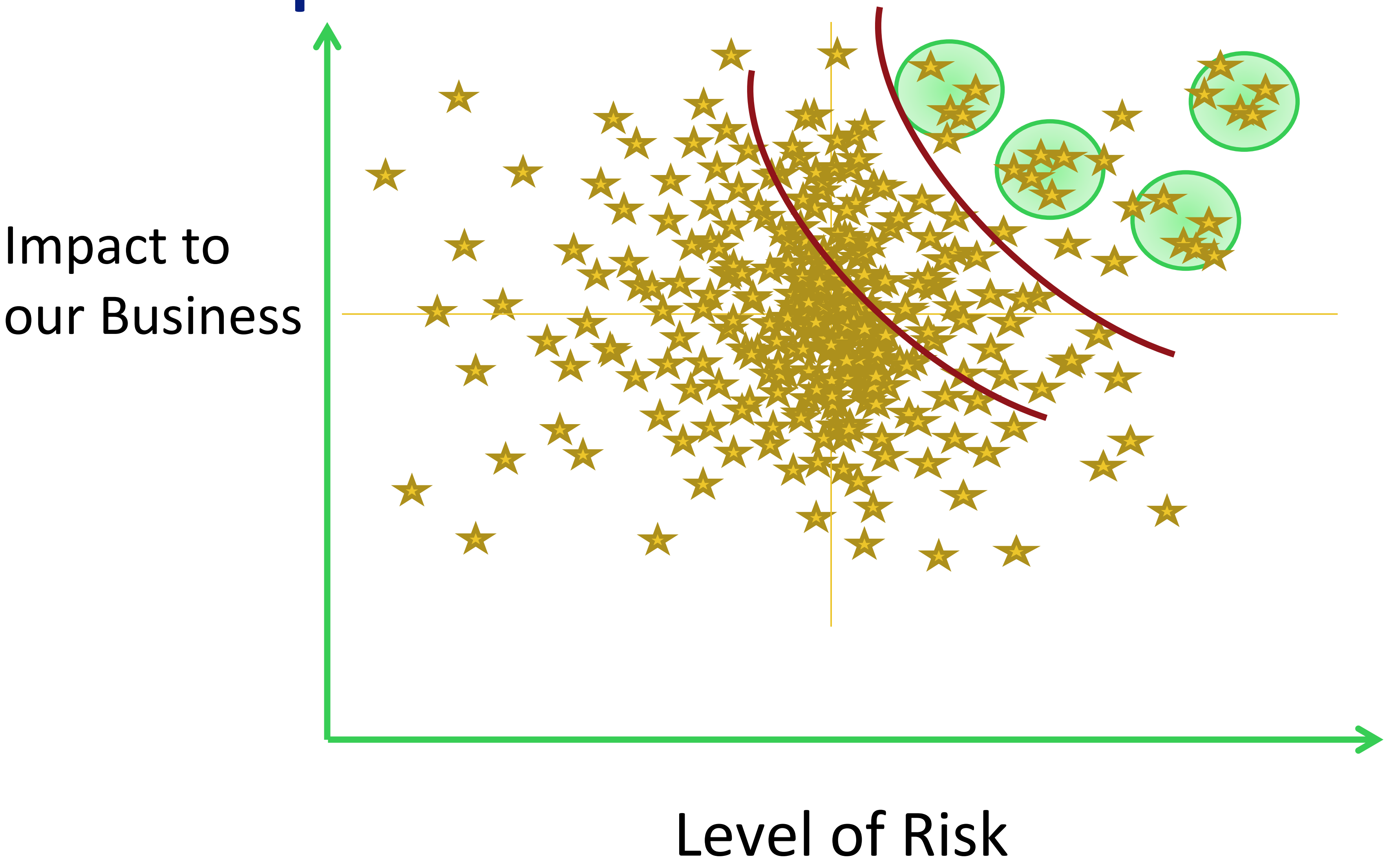
Action 4: Determine What Services Are Critical

- Understand which services you contract on that are critical functions
- Assess the level of risk involved
- Develop a tiering model for the level of risk
- Get alignment on your model from the appropriate senior leadership

Some Sample Services

- Web-Based Applications
  - Are they built securely? Tested? How often? By Whom?
- Network Connectivity
  - Who has access? What can they do? Who validates this?
- Contractors
  - Partner with HR and Legal to review what your policies for employees are and determine how this should differ
  - Background Checks, System Access, other major policies

Risk Map



Action 5: Define Your Tools

- What Tools do you use?
  - Questionnaires
  - On-site Audits
  - Phone Consults with SME’s (Privacy, Architects, etc.)
  - Video Conferencing
  - External Attestations
  - Automated control attestations
  - Third Party Services that review Third Parties
  - Risk-Based Points systems
  - Contracts

Action 6: Develop Your Program

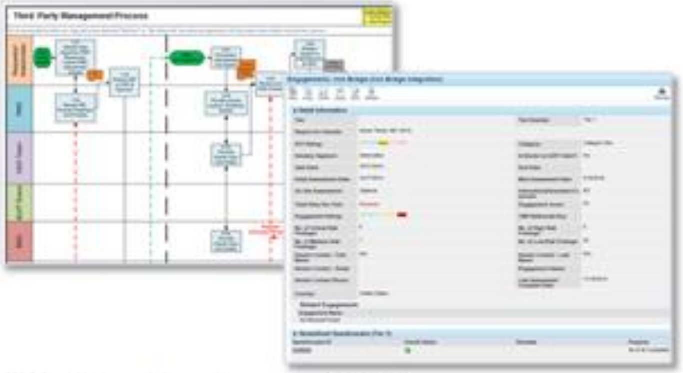
- Define what measures and tools you have/ will develop

- Determine which tools you will use for which tiers of risk

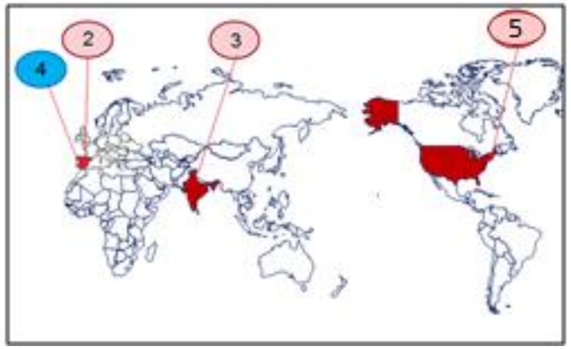
- Get alignment on your program from the appropriate senior leadership

New Tools

- Process Flows and Tracking

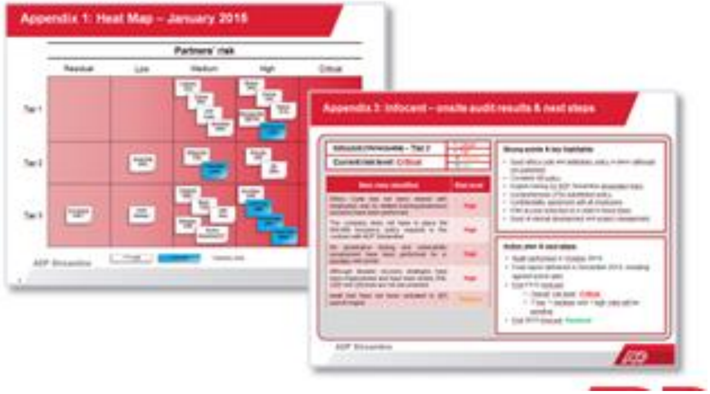


- Global or Business Unit Lens



- Different Tools

- Targeted Reporting and Metrics


Appendix 1: Heat Map – January 2015
Partners' risk
Residual
Low
Medium
High
Critical
Tier 1
Tier 2
Tier 3
Appendix 2: Infocent – onsite audit results & next steps

RSAConference2019
Asia Pacific & Japan

Questions?