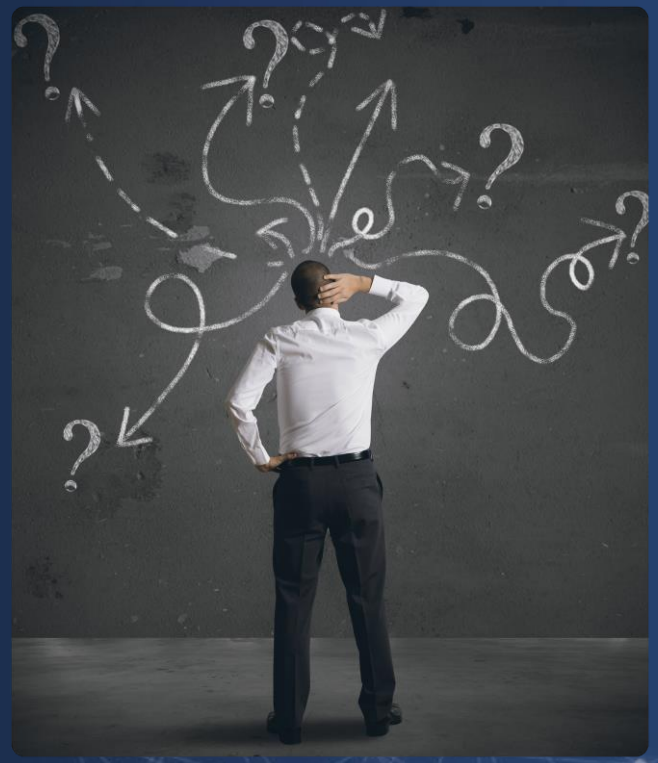
Risk Management Maturity Benchmark Survey 2018

Our 2nd year!

Other maturity models already exist…

…why add another one to the mix?



Existing models are derivatives of CMM

- Most are derivatives of the Capability Maturity Model developed by the Software Engineering Institute in the 1980s
  - Typically use a 0 thru 5 scale
  - Measures the reliability and efficiency of processes

But...

- Reliability and efficiency aren't the same thing as being cost-effective
- Processes are just one part of what makes up a risk management program
  - Policies
  - Processes
  - People
  - Technology

Are these artifacts of a mature RM program?

- The existence of well-documented policies and procedures?
- Essential/fundamental security technologies deployed?
- Active education and awareness program?
- Personnel roles and responsibilities clearly-defined?
- Board of directors engaged and getting regular reports?
- Uses a risk register to track “risks”?
- Risk appetite defined?
- Metrics program in place?

Or is this what maturity looks like?

- Appropriate policies and procedures are clearly defined and documented
- Cost-effective security technologies are providing their intended value
- An effective education and awareness program exists
- Personnel roles and responsibilities are properly defined and staffed
- Board directors are getting the information they need
- A risk register is used to track and report the most important risks
- A clearly defined risk appetite actively drives decision-making
- Meaningful metrics are leveraged to support decision-making

The risk landscape in a nutshell

Complex

Dynamic

Limited Resources

Which means decisions have to be made…

Organizations must excel at prioritizing what they focus on and how they apply their resources.

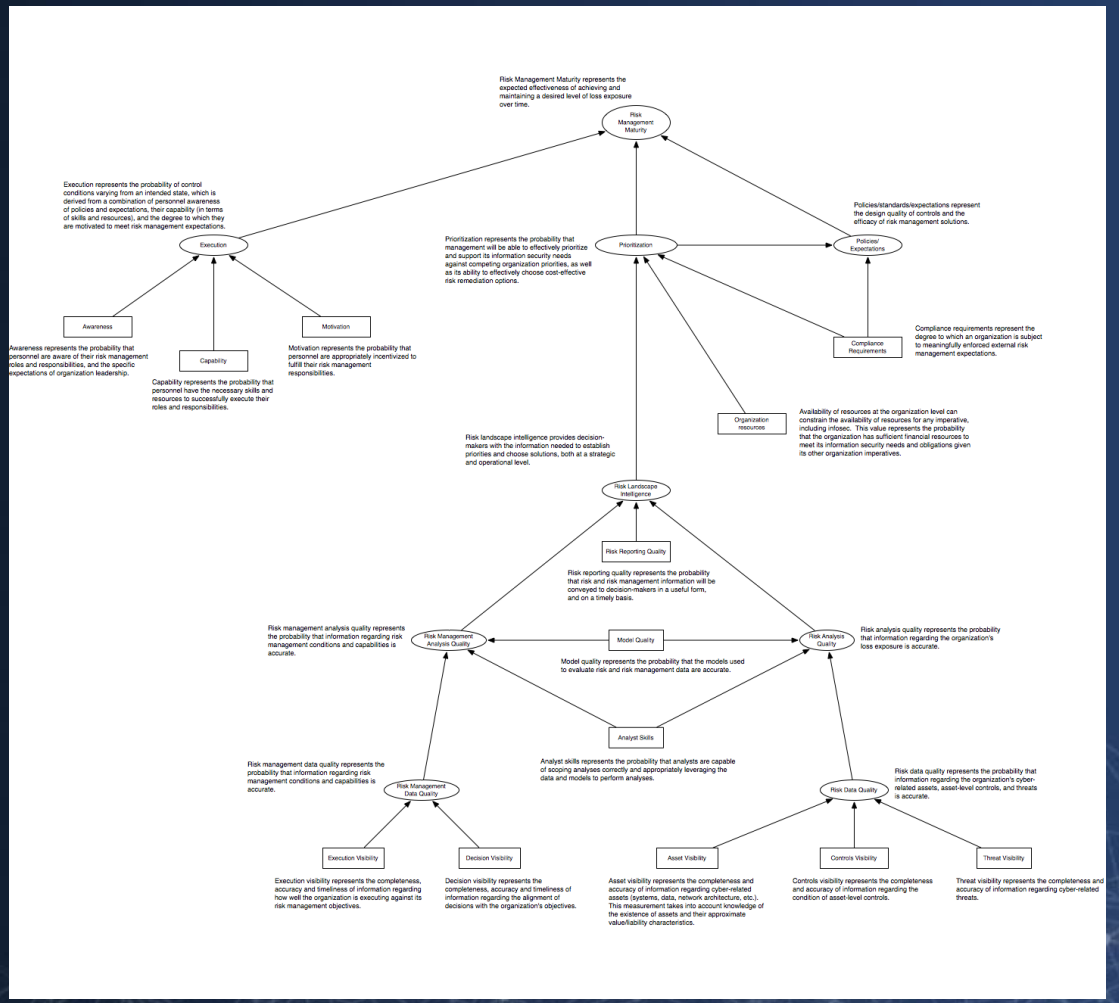
Can we say an organization is “mature” if it…

- Doesn’t know what it’s top risks are?
- Can’t support its risk management investments with cost-benefit analyses?
- Plays whack-a-mole fighting the same problems over and over? For example:
  - Failure to manage patching
  - Inappropriate access privileges
  - Unsanctioned technologies and configurations
  - Shadow IT

FAIR maturity model premise

- Two dimensions to maturity:
  - The ability to make well-informed decisions
  - The ability to execute reliably
- Each of these is decomposed into the factors that drive them, which results in a Bayesian network…

The underlying analytic ontology



The advantage of an underlying ontology…

- Captures the relationships & dependencies between elements
- Results are more likely to be realistic and accurate

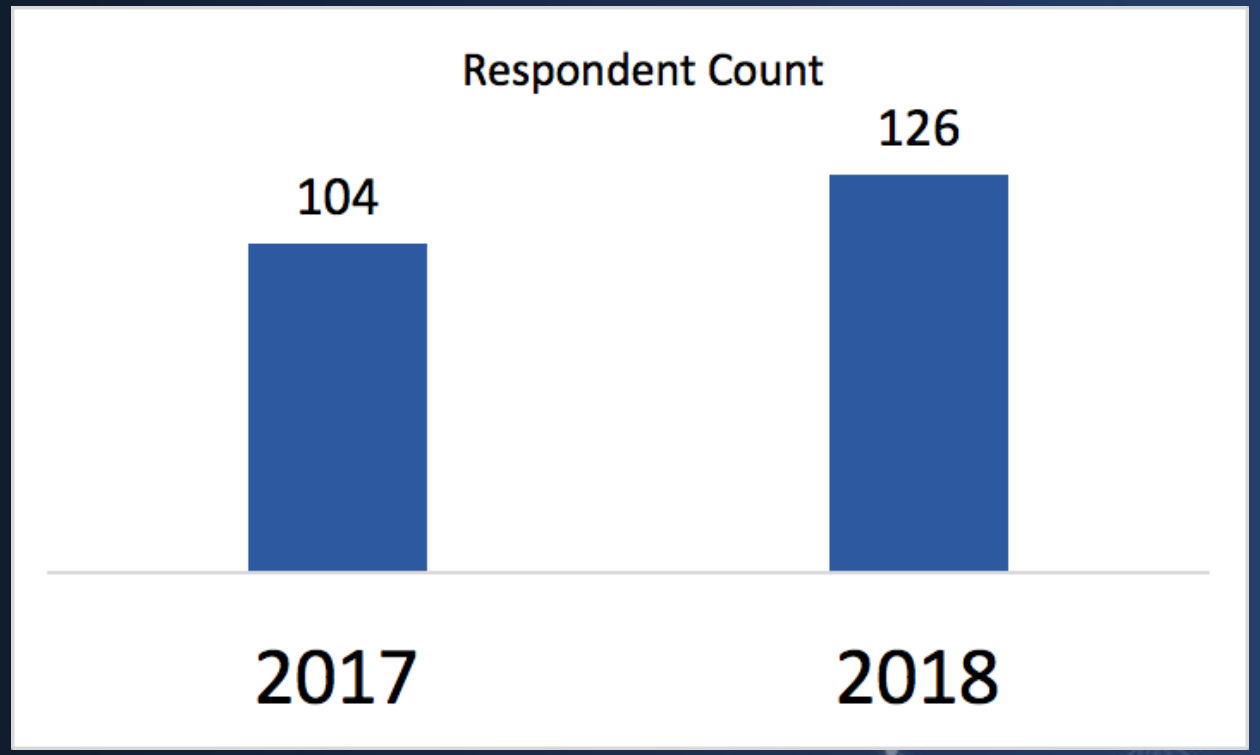
An example question from the survey:

- Which of the following best describes your organization's visibility into its system and information assets?
  - **Strong**: An inventory of systems, applications, and significant information repositories exists and is kept up-to-date through well-defined and consistently practiced procedures. An audit of the inventory would be unlikely to find that more than 5% of the entries are inaccurate.
  - **Partial**: An inventory of systems, applications and significant information repositories exists but is not consistently maintained. Processes for maintaining the inventory are immature or are exercised unreliably. Audits of the inventory regularly find more than 5% of the entries are inaccurate.
  - **Weak**: An inventory of systems, applications, and significant information repositories does not exist or is severely out of date (i.e., cannot be relied on to support decision-making). Processes for maintaining the inventory either do not exist or are not practiced.

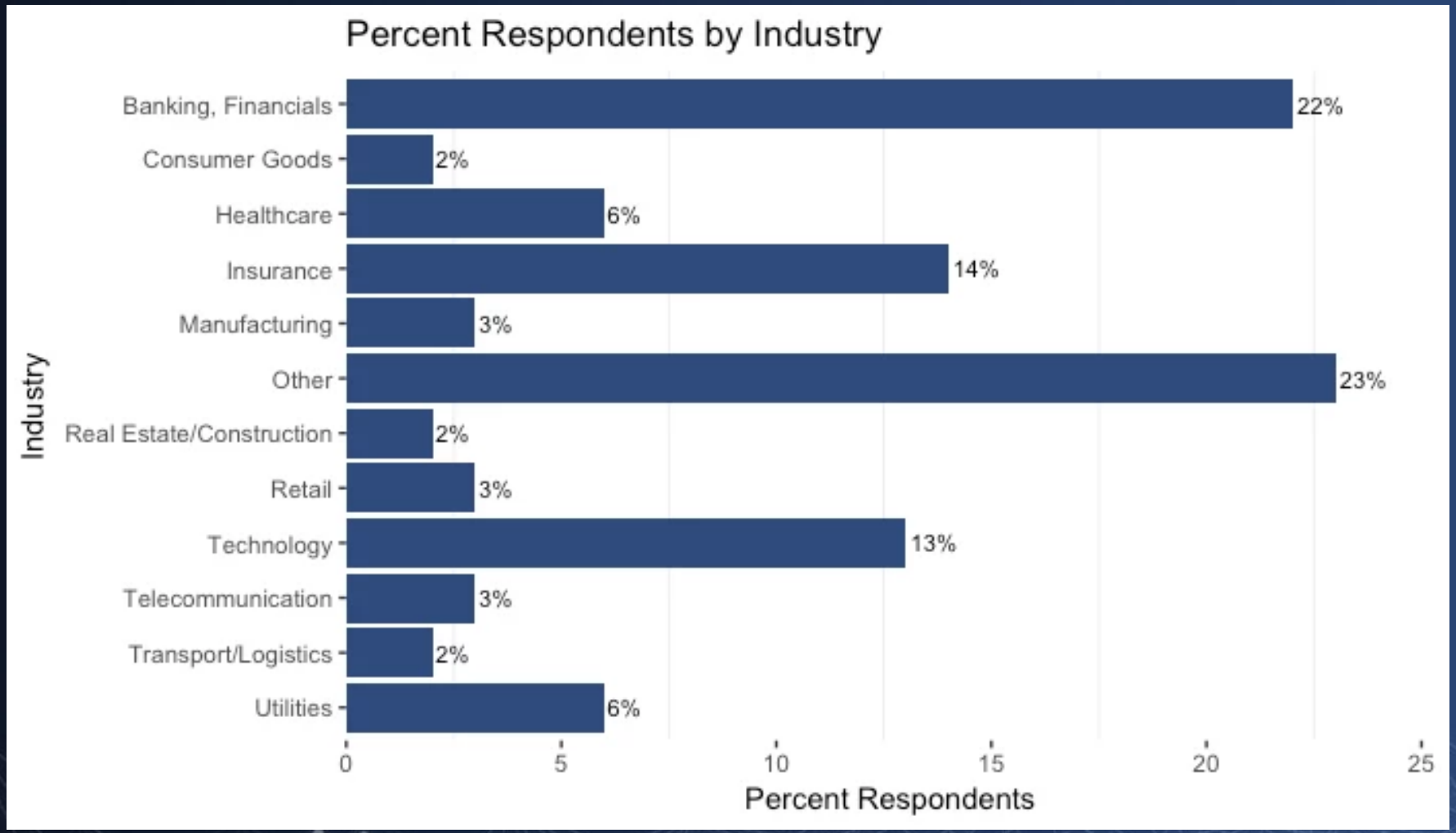
The overall objective is to measure an organization’s ability to cost-effectively achieve and maintain an acceptable level of risk.

Respondent Data

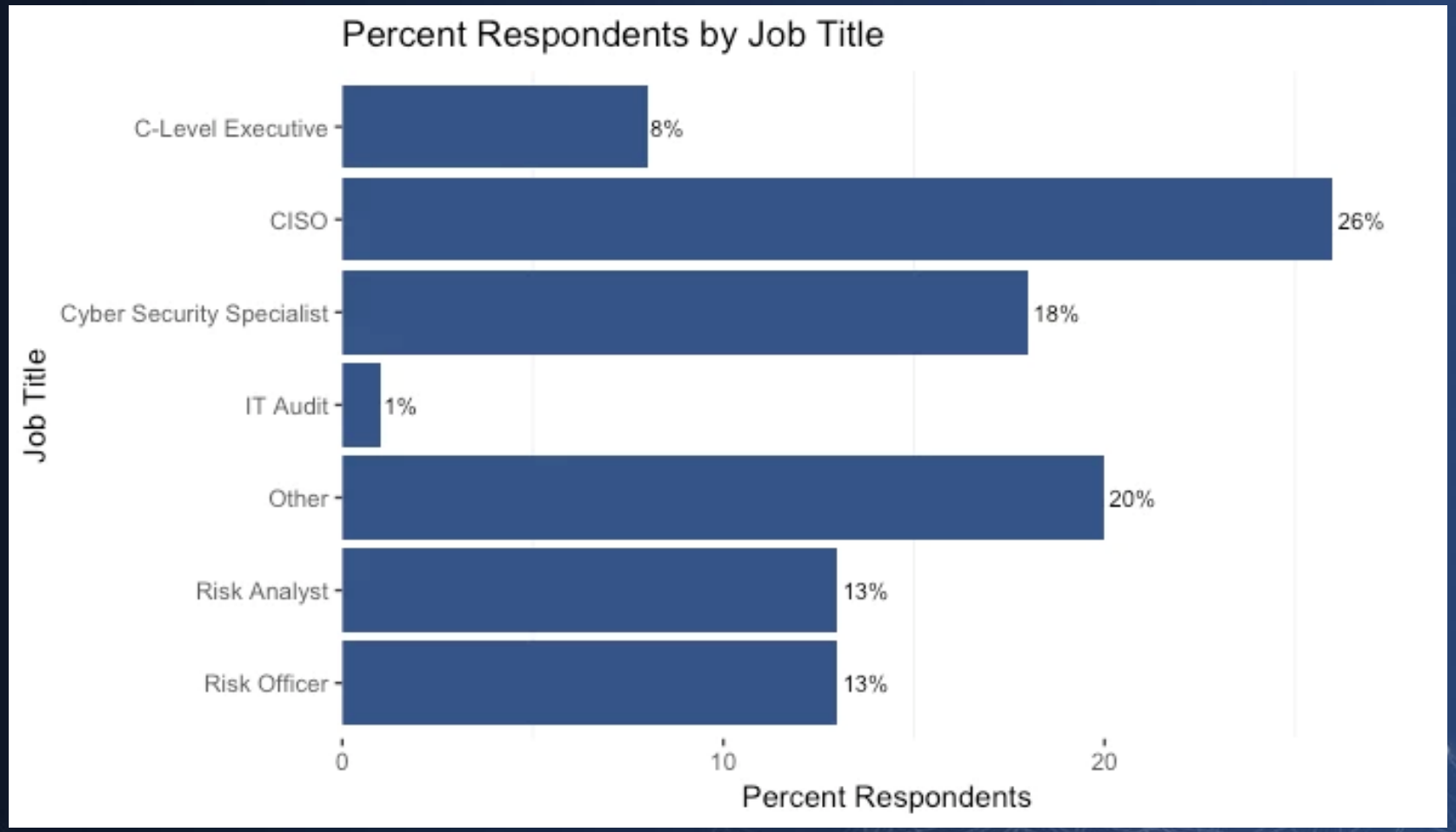
Responses



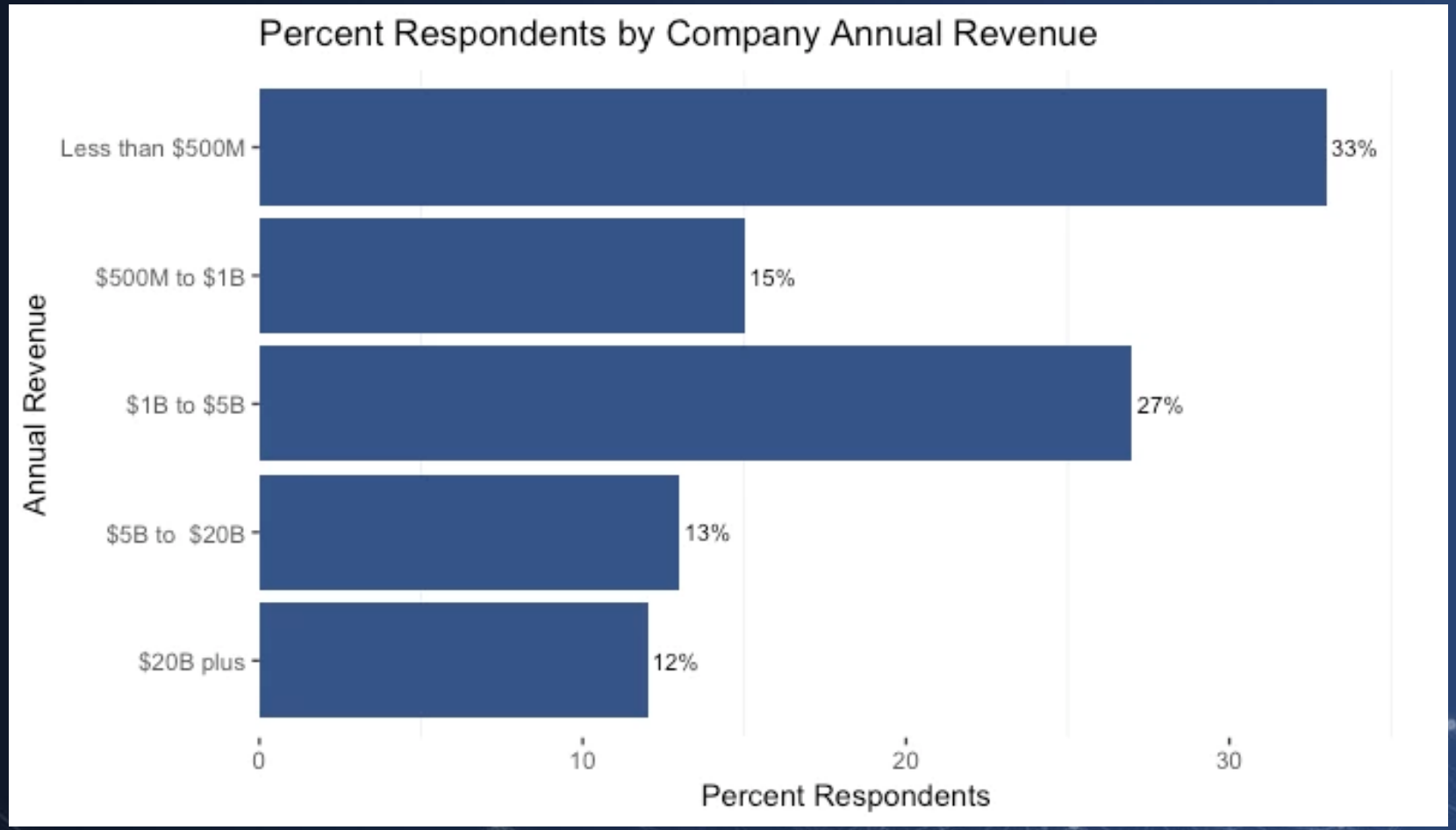
Responses


Percent Respondents by Industry
Industry
Banking, Financials
Consumer Goods
Healthcare
Insurance
Manufacturing
Other
Real Estate/Construction
Retail
Technology
Telecommunication
Transport/Logistics
Utilities
22%
2%
6%
14%
3%
23%
2%
3%
13%
3%
2%
6%
0
5
10
15
20
25
Percent Respondents

Responses

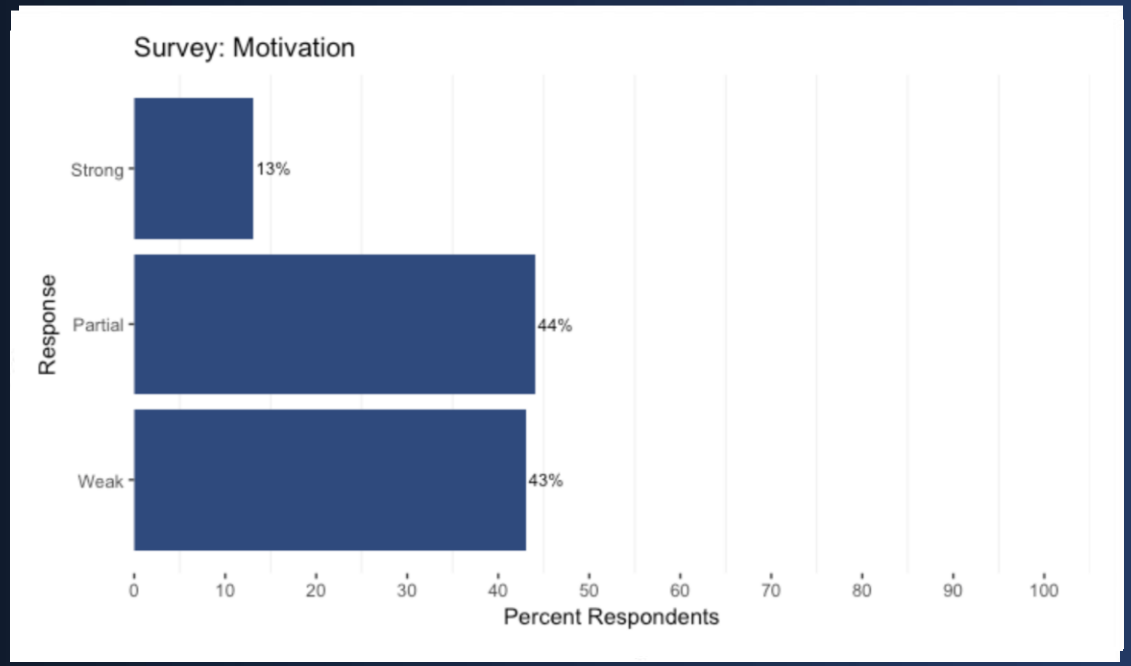

Percent Respondents by Job Title
C-Level Executive
CISO
Cyber Security Specialist
IT Audit
Other
Risk Analyst
Risk Officer
8%
26%
18%
1%
20%
13%
13%
Job Title
0
10
20
Percent Respondents

Responses


Percent Respondents by Company Annual Revenue
Annual Revenue
Less than $500M
$500M to $1B
$1B to $5B
$5B to $20B
$20B plus
33%
15%
27%
13%
12%
0
10
20
30
Percent Respondents

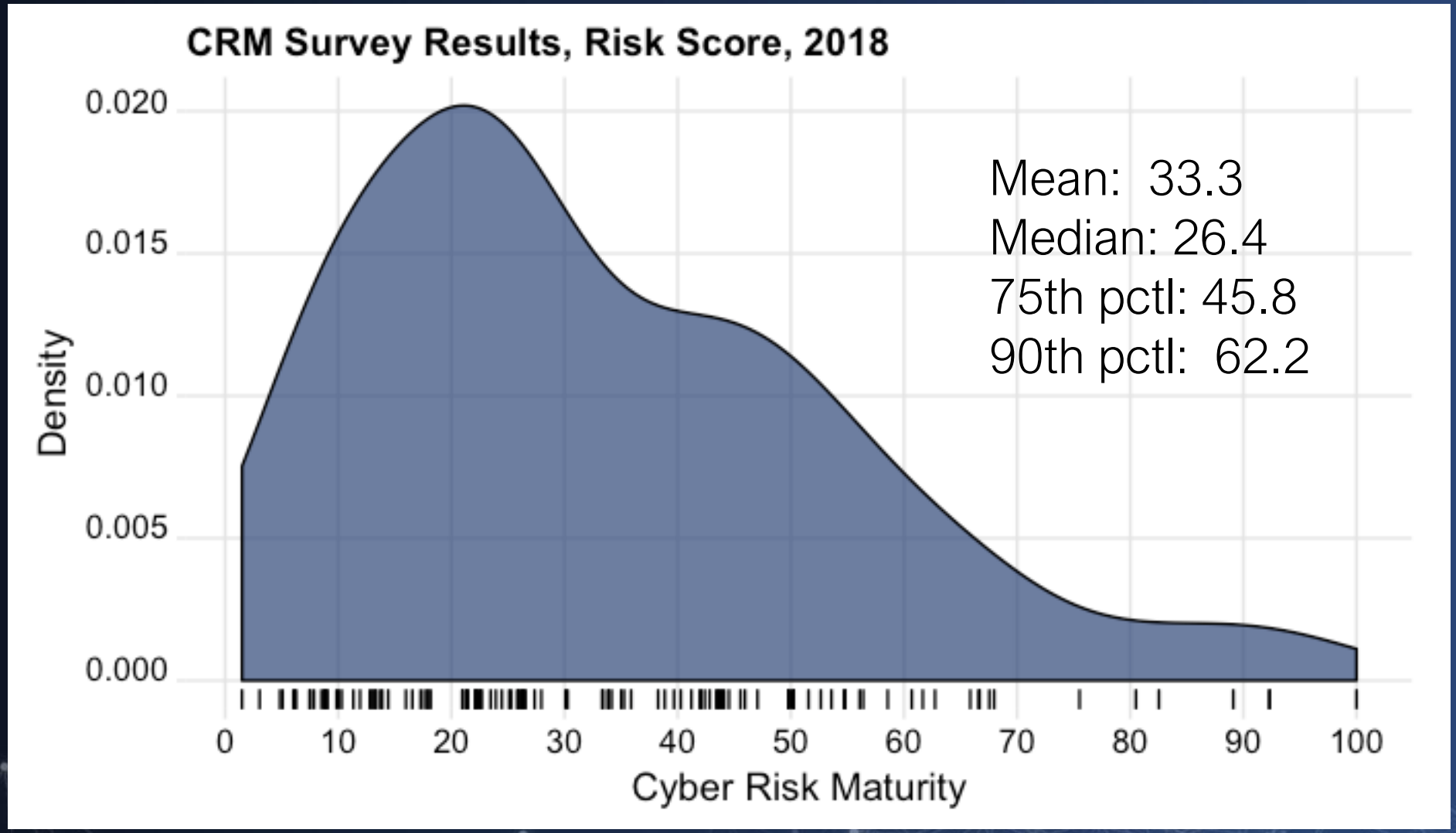
Results

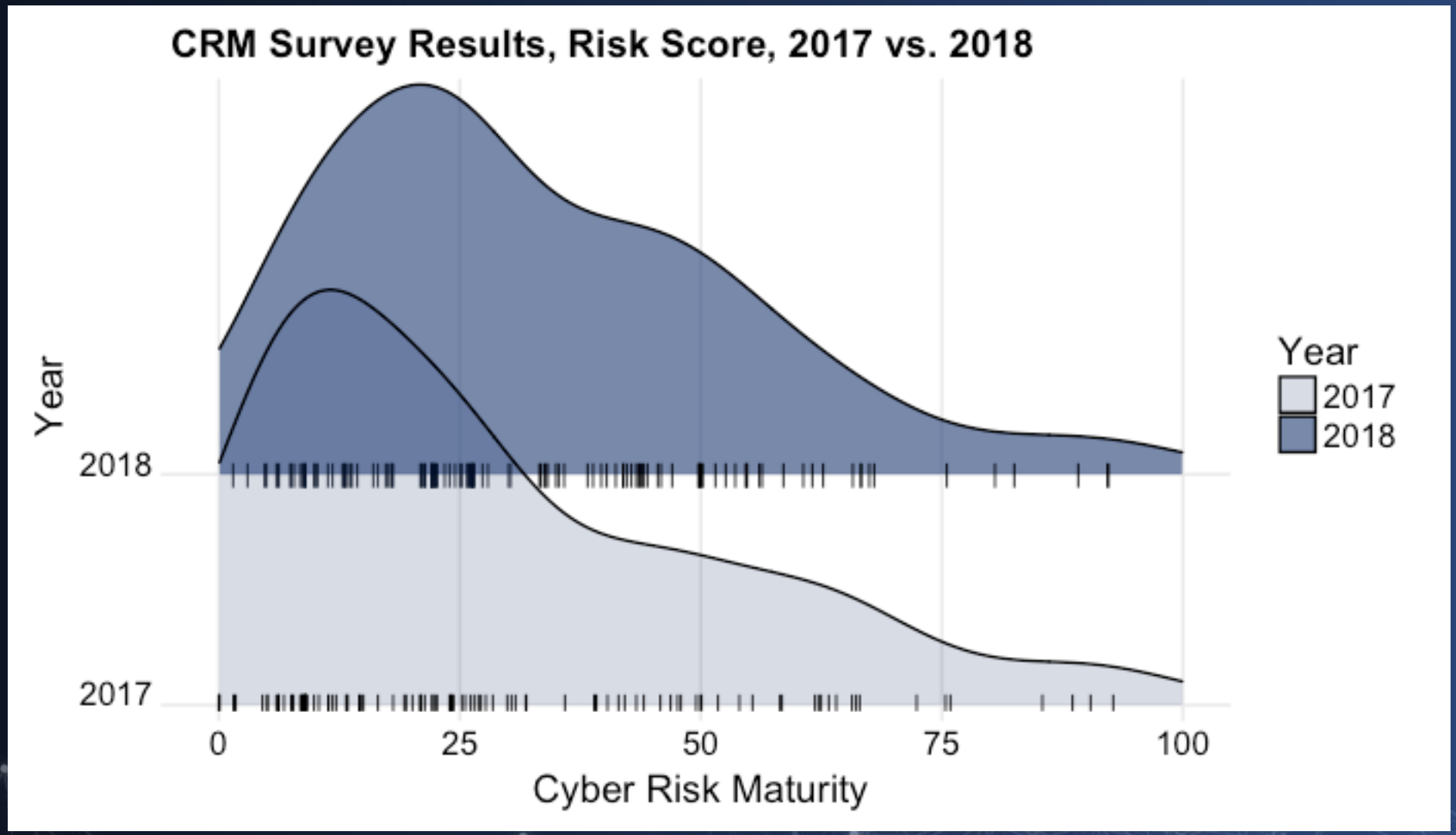
Results for each survey element…

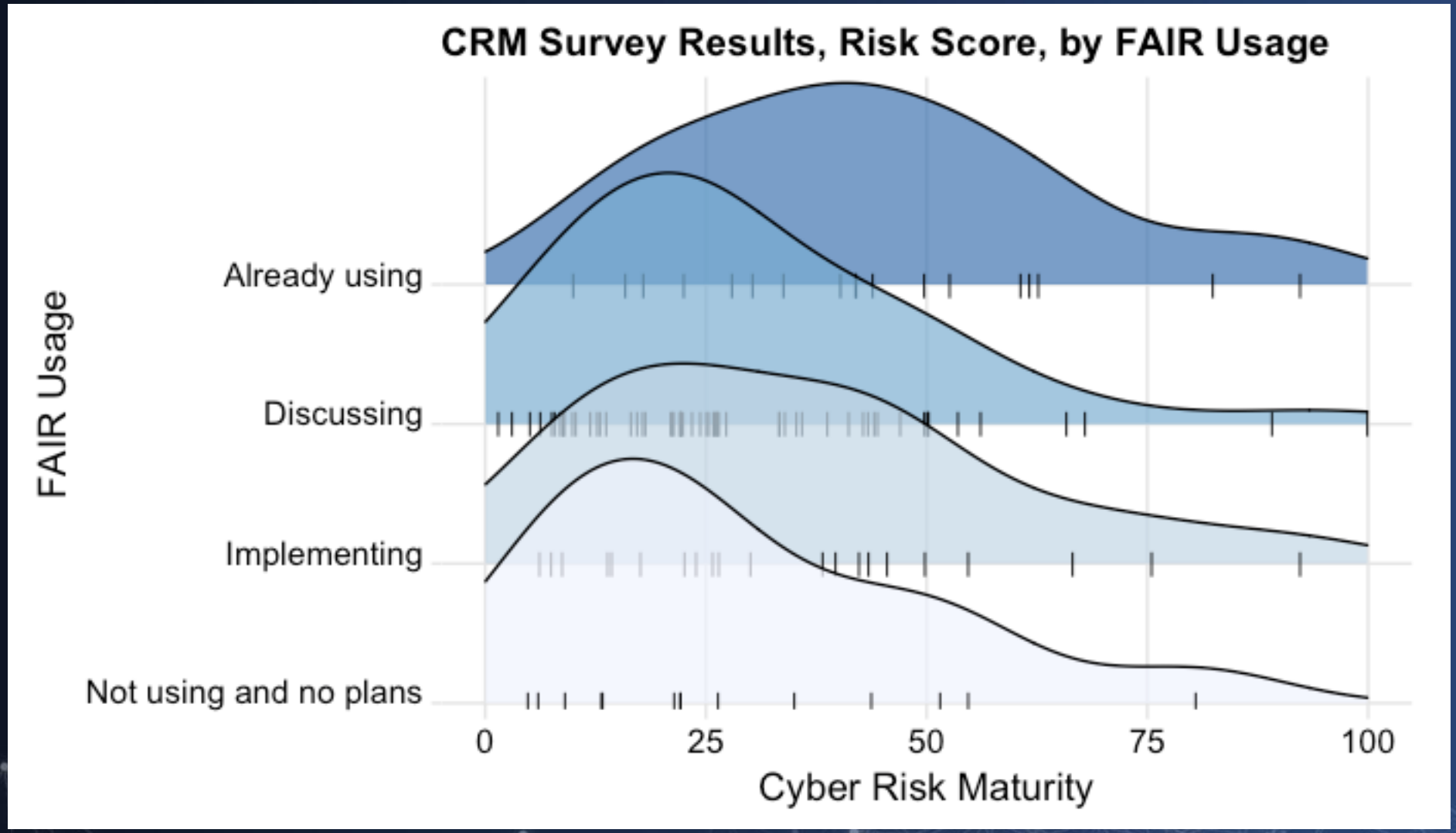


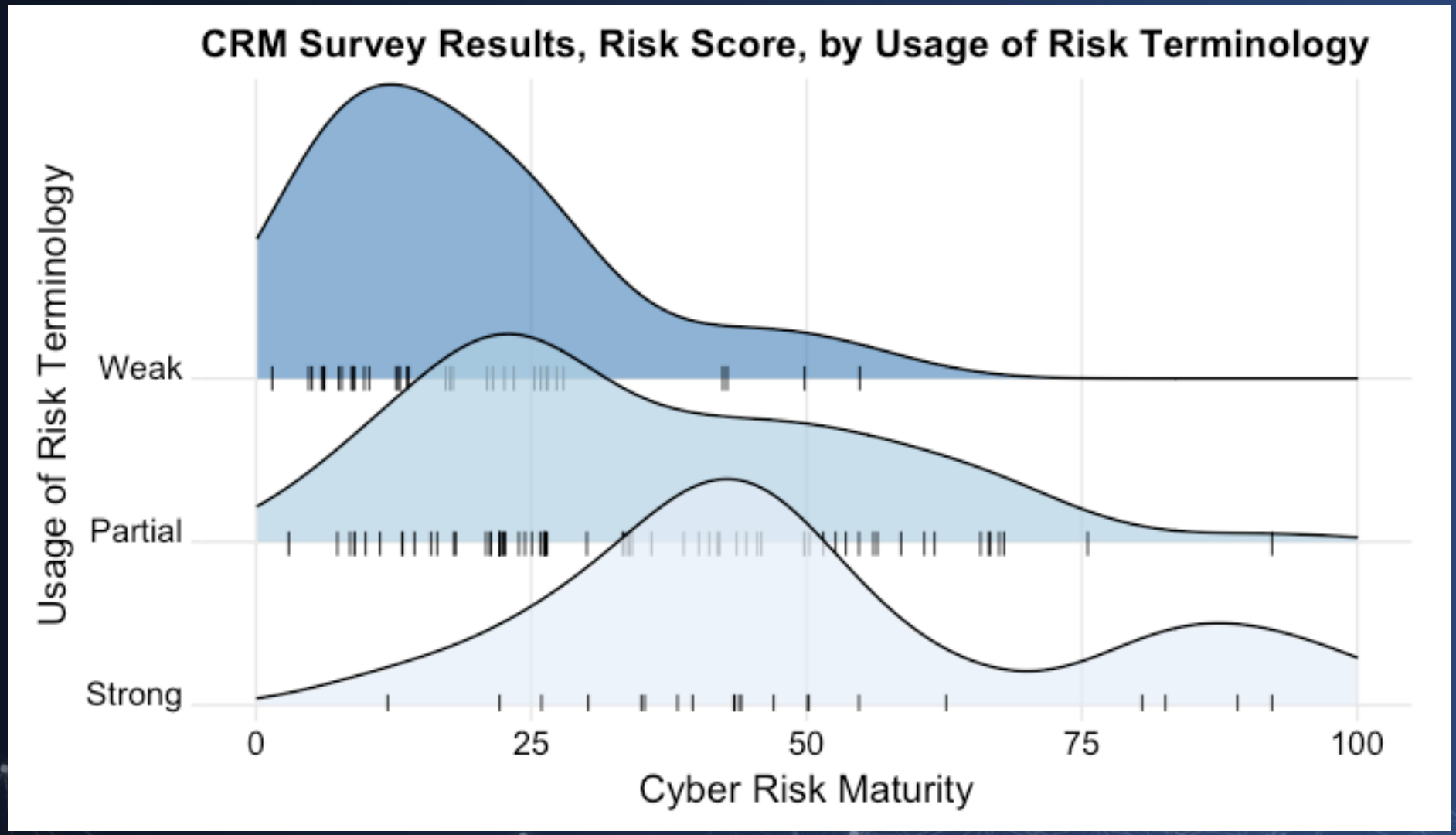
Scoring model

- For each organization, translated results from the Bayesian model into a score between 0 and 100
- Represents (very roughly) the probability that an organization can cost-effectively achieve and maintain an acceptable level of risk


CRM Survey Results, Risk Score, 2018
Density
0.020
0.015
0.010
0.005
0.000
0
10
20
30
40
50
60
70
80
90
100
Cyber Risk Maturity
Mean: 33.3
Median: 26.4
75th pctl: 45.8
90th pctl: 62.2


CRM Survey Results, Risk Score, 2017 vs. 2018
Year
2018
2017
0
25
50
75
100
Cyber Risk Maturity
Year
2017
2018


CRM Survey Results, Risk Score, by FAIR Usage
FAIR Usage
Already using
Discussing
Implementing
Not using and no plans
0
25
50
75
100
Cyber Risk Maturity


CRM Survey Results, Risk Score, by Usage of Risk Terminology
Usage of Risk Terminology
Weak
Partial
Strong
0
25
50
75
100
Cyber Risk Maturity

Benchmark results summary…

- For the responding population:
  - The bad news: the ability to make well-informed decisions and/or execute reliably is generally very low
  - The good news: there appears to be improvement (although minimal) from 2017 to 2018

Panel discussion…