RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CXO-W10

Defining a Risk Appetite That Works

Jack Jones
Chairman - FAIR Institute

What we'll cover…

- Appetite vs. tolerance — what's the diff?
- Why bother?
- Comparing risk appetite definitions
- An example of a "working" risk appetite
- Getting aligned with your risk appetite
- Staying aligned with your risk appetite
- Applying this where you work
- Q&A

Example #1: What's your risk appetite?

IT DEPENDS…

Risk appetite is always a function of balancing need/desire, cost, and risk
— which can vary over time

Appetite vs. Tolerance — What's the diff?

A LINE IN THE SAND VS. BEHAVIOR MODIFICATION

You have to define the former before you can deal with the latter

Why bother?

- Provide clarity in expectations
- Improve focus in risk management efforts
- Improve communication with stakeholders
- Reduce the likelihood of unacceptable loss
  - What's an "unacceptable loss"?

RSAConference2019

Comparing risk appetite definitions

Is this a useful risk appetite statement?

"The organization has zero appetite for the loss of customer data"

- ~~Realistic & actionable?~~
- Provides clarity in expectations?
- Improves focus in risk management efforts?
- Improves communication with stakeholders?
- Reduces the potential for unacceptable loss?

Is this a useful risk appetite statement?

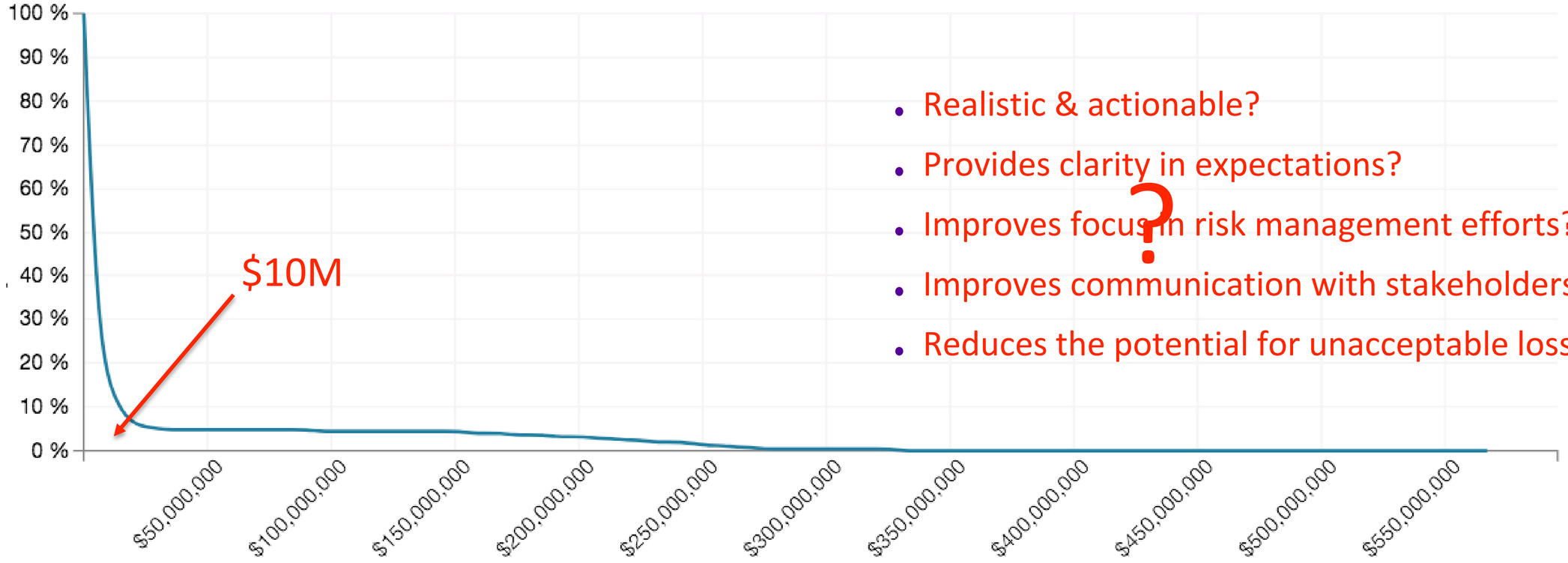
"The organization has a low appetite for the loss of customer data"

- Realistic & actionable?
- ~~**Provides clarity in expectations?**~~
- Improves focus in risk management efforts?
- Improves communication with stakeholders?
- Reduces the potential for unacceptable loss?

Expressing it economically

"The organization does not want to exceed $10M in loss."

Aggregate?
Single event?



- Realistic & actionable?
- Provides clarity in expectations?
- Improves focus in risk management efforts?
- Improves communication with stakeholders?
- Reduces the potential for unacceptable loss?

?

…or…

RSAConference2019

An example of a “working” risk appetite

Step 1

- Choose a risk (loss event scenario) to set an appetite for, for example:
  - Disclosure of customer PII records
  - Business process outage
  - Regulatory non-compliance
  - Financial misstatement
  - etc…

Our example…

Yes, this means you may define multiple risk appetites

Step 2

- Define a loss magnitude threshold for that risk, for example:
  - No disclosure of > 1M customer PII records
- Why 1M records?
  - Reduces the number of systems/applications to a manageable number
  - Losing “millions of records” has a subjective sting to it
  - No, it isn’t materially different than 999k records, but you have to draw the line somewhere

NOTE: You can lower the threshold later — after the organization has reliably established success at this level

Step 3

- Define a probability threshold, for example:
  - Quantitative: < 5% (within the next 12 months)
  - Qualitative: Very Low (within the next 12 months)
    - How do you define “Very Low”?

This is the probability of an event that exceeds the loss magnitude threshold defined in step 2

Example of "Very Low" probability criteria (malicious breach context)

- Defined by combining characteristics of the threat landscape with control conditions, for example:

- For assets containing > 1M customer PII records:
  - Assets and privileged systems* that ARE directly Internet-facing
    - No more than 1 exploitable condition** every three years (control deficiencies)
    - All exploitable conditions discovered and remedied within 48 hours
  - Assets and privileged systems that ARE NOT directly Internet-facing
    - No more than 2 exploitable conditions per year (control deficiencies)
    - Exploitable conditions discovered and remedied within 7 days

Requires policies & processes that limit the likelihood of introducing new exploitable conditions

Requires policies, processes, and technologies that enable rapid detection and remediation of problems

* "Privileged systems" are systems used by personnel with privileged access to "crown jewels".

** "Exploitable conditions" are those weaknesses that permit an attacker to directly affect the assets at risk (e.g., a SQL injection flaw, weak password, etc.)

…results in the following risk appetite definition

"Less than a 5% (or, "Very Low") probability in the next 12 months of a disclosure of > 1M customer PII records"

- Realistic & actionable?
- Provides clarity in expectations?
- Improves focus in risk management efforts?
- Improves communication with stakeholders?
- Reduces the potential for unacceptable loss?

Example outage-related appetite

Less than a 5% probability in the next 12 months of > 100k lost customer transactions in any 24 hour period

Example regulatory commpliance-related appetite

Less than 5% probability in the next 12 months of a cybersecurity related regulatory action against the company (e.g., consent decree)

Example financial reporting-related appetite

Less than 5% probability in the next 12 months of a financial misstatement > $10M that stems from an IT or cyber-related problem.

Definition criteria summary - the appetite must…

- Be realistic and actionable
- Be aligned to a specific type of loss event
- Clearly describe a severity threshold
- Clearly describe a probability threshold for a specific timeframe (e.g., next 12 months)

So, you've defined your risk appetite(s) — now what?

Two things to focus on…

1. Getting aligned with the appetite
2. Staying aligned with the appetite

RSAConference2019

Getting aligned with your risk appetite

Getting aligned boils down to…

1. Identify assets that constitute “crown jewels” within the context of the appetite
   - A “crown jewel” is anything that, if adversely affected in the manner described by the appetite definition (e.g., disclosure, outage, etc.), exposes the organization to loss that exceeds the magnitude threshold
2. Evaluate current probability of exceeding the appetite’s magnitude threshold (given the threat landscape and control conditions)
3. If/where probability exceeds appetite(s), identify and implement options for aligning with the appetite(s)

Example — identifying PII-related crown jewels

- Crown jewels (contain or process more than 1M customer PII records)
  - 5 production databases
  - 2 test/dev databases
  - 14 production applications
  - 5 test/dev applications
  - 22 production servers
  - 9 test/dev servers
  - 3 servers containing old data dumps
- Privileged systems
  - 24 personnel w/ privileged access to production crown jewels (dbas, sysadmins, etc.)
  - ~150 personnel w/ privileged access to test/dev crown jewels (dbas, sysadmins, developers, test engineers, etc.)

Identify easy opportunities for PII appetite alignment

- Skinny-down the number of records in dev/test to eliminate those systems from the list of crown jewels and privileged systems
- Remove old data dumps

Next alignment steps

1. Which PII crown jewels and privileged systems are Internet-facing?
   - Identify and fix any exploitable conditions
2. Which PII crown jewels and privileged systems are not Internet-facing?
   - Identify and fix any exploitable conditions

RSAConference2019

The hard part — staying aligned with your risk appetite

Two dimensions to staying within appetite…

- Setting decision-making boundaries (policies, authorities, etc.)
  - Help people avoid doing “stupid stuff”
- Establishing early-warning indicators (KRIs & KPIs)
  - Identify and correct appetite violations

Setting decision-making boundaries

- Example policies, standards, and processes
  - 100% of asset management information regarding crown jewels and privileged systems must be accurate at all times
  - No crown jewels permitted in dev/test environments
  - No third parties may have > 1M customer records
  - Any proposed additional crown jewel must:
    - Be reviewed by the CISO and approved by the CIO and the information owner before being implemented
    - Comply with crown jewel control standards
  - Policy exception requests that affect crown jewels and relevant privileged systems require approval by the information owner and a direct report of the CEO (e.g., COO)
  - Personnel with privileged access to crown jewels must pass an examination that demonstrates an understanding of their risk management responsibilities

Example Cyber KRIs - 4th Qtr

	KRIs	Threshold	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Trend
Threats	Phishing attempts against **crown jewel** privileged personnel	20% increase	2	0	1	1	
	Scans/probes of Internet-facing **crown jewels**	20% increase	10	8	9	14	
	Illicit activity against non-Internet-facing **crown jewels**	Any activity	0	0	0	0	
	Malware infections requiring intervention	20% increase	20	45	18	15	
	Phishing campaigns directed at the organization	20% increase	3	2	5	7	
	Concerted website attacks	30% increase	5	7	8	8	
	DoS attacks	50% increase	0	1	2	2	
Assets	# Shadow IT environments containing **crown jewels**	0	24	24	22	15	
	# Internet-facing **crown jewels**	Any increase	1	1	1	1	
	# Legacy systems that are **crown jewels**	0	3	3	2	1	
	# of legacy systems unable to meet security requirements	15	4	5	5	6	
	# of "critical" 3rd parties w/ low security scores	5	15	11	10	9	
Key Controls	# of **crown jewels** w/ substandard security controls	0	9	8	6	3	
	# of personnel with privileged access to **crown jewels**	50	471	423	166	49	
	# of policy exceptions on **crown jewels**	5	9	5	6	5	
	# of **crown jewel** systems unable to meet recovery requirements	0	12	12	7	5	
	# of user accounts w/ inappropriate access	20	123	85	43	12	
	# of systems/databases w/ non-compliant passwords	5	29	34	21	11	
	# of systems missing critical patches	60	50	35	120	57	
	Average time to detect compromise (days)	2	30	35	28	1	
	# of systems/applications that failed recovery testing	10	8	5	6	9	

FAIR INSTITUTE

Example Cyber KPIs - 4th Qtr

	Risk Management KPIs	Threshold	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Trend
Decision Support	% of **crown jewels** with up-to-date information in the CMDB	100%	50%	55%	75%	92%	
	% of **crown jewels** with advanced controls monitoring in place and operational	100%	50%	70%	90%	100%	
	% of **crown jewels** with comprehensive threat detection deployed and operational	100%	50%	75%	90%	97%	
	% of non-compliant conditions on **crown jewels** with root cause analysis performed	100%	0%	50%	80%	100%	
	% of environment with basic threat detection in place and operational	75%	30%	45%	50%	65%	
	% of environment with basic controls monitoring in place and operational	75%	30%	40%	55%	70%	
	% of loss events with root cause analysis performed	90%	10%	25%	60%	93%	
	% of all non-compliant conditions with root cause analysis performed	30%	0%	0%	20%	30%	
	% of risk analyses that undergo peer review	20%	0%	10%	20%	20%	
	% of network scanned monthly for sensitive information	75%	20%	40%	55%	70%	
	% of policies reviewed within the past 12 months	30%	25%	30%	30%	30%	
Execution	% of security, audit, and regulatory **crown jewel** findings closed on time	100%	30%	40%	80%	95%	
	% of **crown jewel** critical patch deployments within SLA	100%	25%	50%	80%	90%	
	% of user access privilege updates within SLA	90%	70%	80%	95%	95%	
	% of systems/applications with compliant administrative passwords	95%	65%	75%	80%	90%	
	% of systems with up-to-date malware detection	90%	85%	95%	95%	93%	
	% of risk analyses that pass peer review	90%	50%	75%	95%	90%	
	% personnel passing phishing test exercises	80%	30%	50%	65%	75%	
	% developers, sysadmins, and DBAs up-to-date on training	90%	0%	50%	75%	80%	
	% of audit, regulatory and other findings closed on time	90%	30%	40%	80%	95%	

FAIR INSTITUTE

Example Board Reporting - 4th Qtr

Four risk types, their appetite thresholds, and alignment condition over time.

Top Risks

Top Risks	Event Magnitude Threshold	Probability Threshold	Probability Levels 1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	Trend
Critical System Outage	100k lost transactions	5%	7%	7%	5%	3%	
Customer Information Breach	1M records	5%	10%	8%	8%	6%	
Regulatory Non-compliance	Regulatory action	5%	5%	5%	3%	3%	
Financial Misstatement (IT related)	> $10M	5%	3%	3%	3%	3%	

Represents the probability of an event in the next 12 months that exceeds the magnitude threshold.
Excludes assets that are not known about or are not centrally managed (shadow IT).

If preferred, you can use qualitative labels like “Very Low” (green), “Low” (yellow), etc. instead of %’s

FAIR INSTITUTE

Simply being explicit in your expectations and intentions can have a significant effect on focus and efficacy.

RSAConference2019

Applying what you've learned

In the next week…

- Begin to socialize this approach with colleagues
  - Identify their concerns and listen to their ideas
- If “risk appetite” is too sensitive a term where you work, you can refer to this approach as “crown jewel focused risk management”
  - But make no mistake: what the organization defines as a “crown jewel” and the steps it takes to manage them (or not manage them) is a reflection of both its risk appetite and risk management maturity

In the next 30 days…

- Get stakeholder support for applying this approach (or your variation)
  - Propose a hypothetical appetite for one or more types of risk
  - Describe how the organization could leverage it to improve risk management
    - Providing clearer expectations
    - Improving focus
    - Improving communication
    - **Reducing the organization's exposure to extreme events**

In the next 90 days…

- Once you have the go-ahead, begin defining and leveraging your first risk appetite
  - Find out what type of risk (e.g., outage, breach, etc.) management cares most about
  - Work with stakeholders to define an initial appetite for that risk type
  - Resist the urge to set too low an initial appetite
  - Focus first on getting the organization aligned with the initial appetite
  - Focus second on how to help the organization stay within the initial appetite
  - Build on your initial success to define and leverage appetites for other risk types
  - Consider lowering your risk appetite over time

RSAConference2019

Q&A