RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century

Rick Howard
CSO
Palo Alto Networks
@raceBannon99

David Caswell
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century

Rick Howard
CSO
Palo Alto Networks
@raceBannon99

David Caswell
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century

Rick Howard

CSO
Palo Alto Networks
@raceBannon99

David Caswell

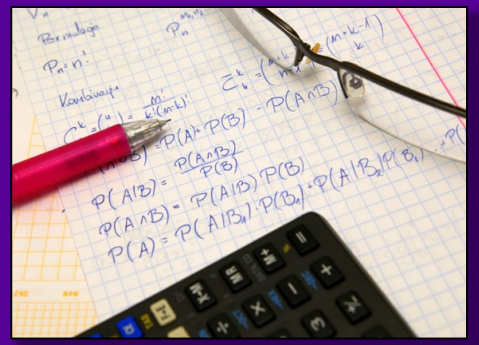
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century



Rick Howard

CSO
Palo Alto Networks
@raceBannon99

David Caswell

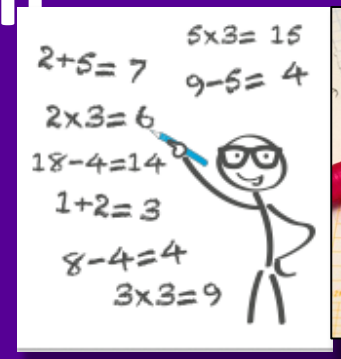
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

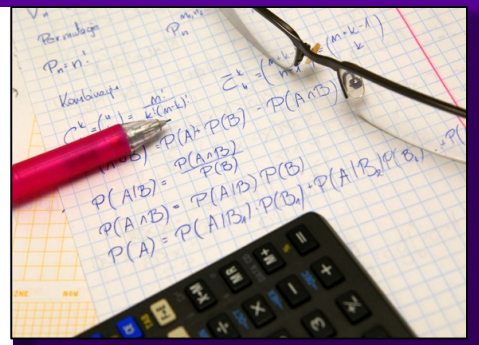
RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century





Rick Howard

CSO
Palo Alto Networks
@raceBannon99

David Caswell

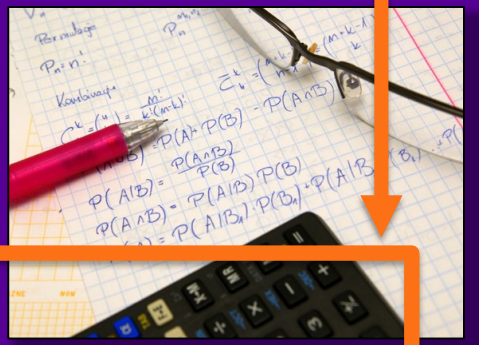
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: GRC-T06

Superforecasting II: Risk Assessment Prognostication in the 21st century



Rick Howard
CSO
Palo Alto Networks
@raceBannon99

David Caswell
Permanent Professor and Head, Department of Computer and Cyber Sciences
United States Air Force Academy

We Talked about …

We Talked about …

Books to Read

We Talked about …

Books to Read

Heat Maps are Bad Science

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

Bayes & Monte Carlo History

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

Bayes & Monte Carlo History

How to think about Superforecasting

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

Bayes & Monte Carlo History

How to think about Superforecasting

Getting Ready for the Board

paloalto NETWORKS

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

Bayes & Monte Carlo History

How to think about Superforecasting

Getting Ready for the Board

paloalto NETWORKS

We Talked about …

Books to Read

Heat Maps are Bad Science

What CISOs know about Probability is Likely Wrong

Bayes & Monte Carlo History

How to think about Superforecasting

Getting Ready for the Board

Replace Heat Maps with Latency Curves

How to Build Latency Curves

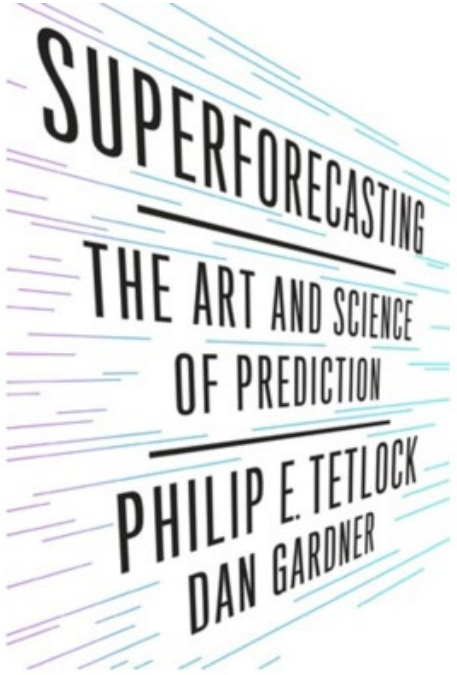
paloalto NETWORKS

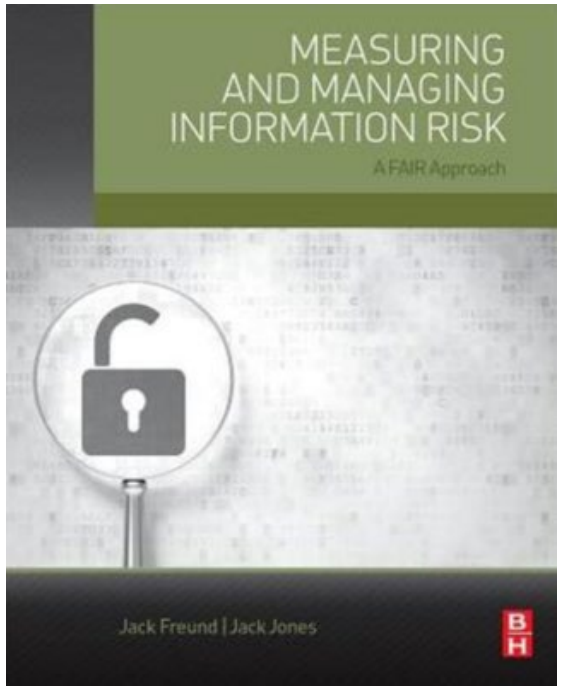
Transition

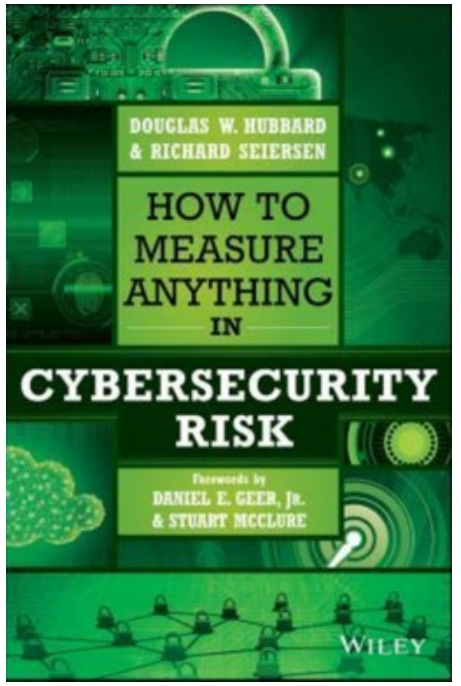
RSAConference2019

Books to Read

Why this Talk?



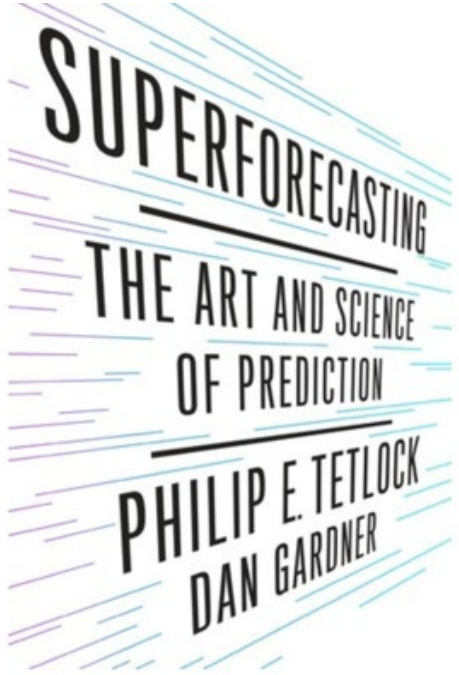




CYBERSECURITY
CANON

https://cybercanon.paloaltonetworks.com/

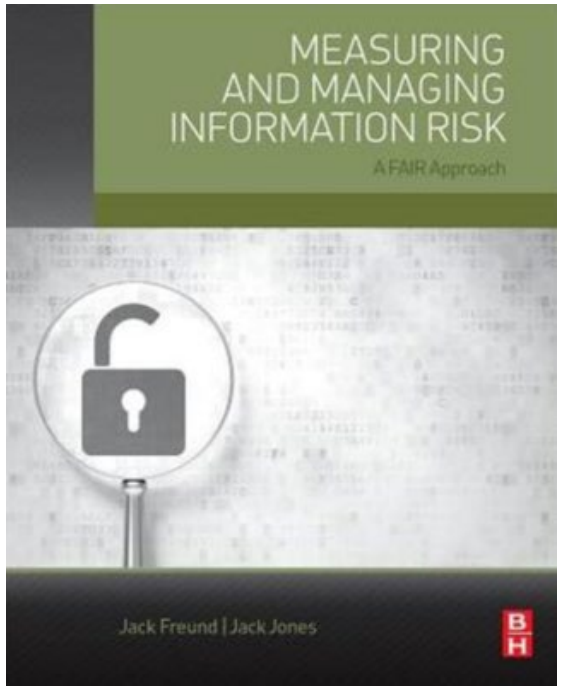
Why this Talk?

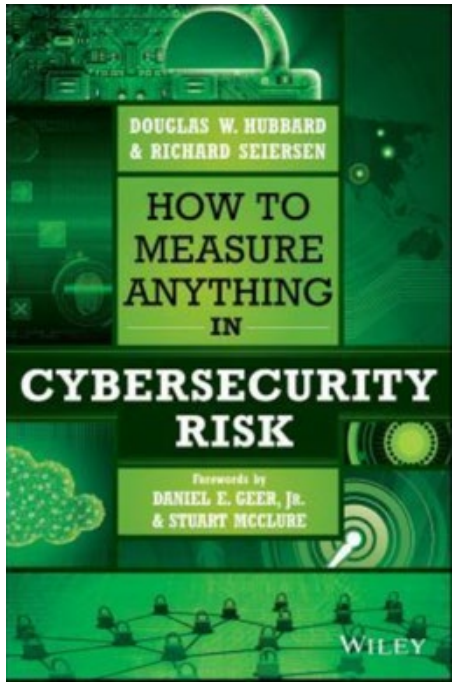


Philip Tetlock

Dan Gardner

Why this Talk?





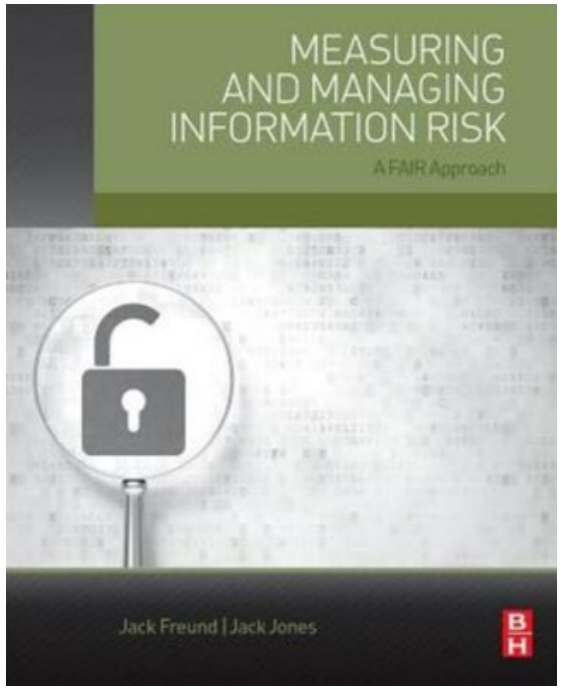
CYBERSECURITY
CANON

https://cybercanon.paloaltonetworks.com/

Why this Talk?

Jack Jones

Jack Freund



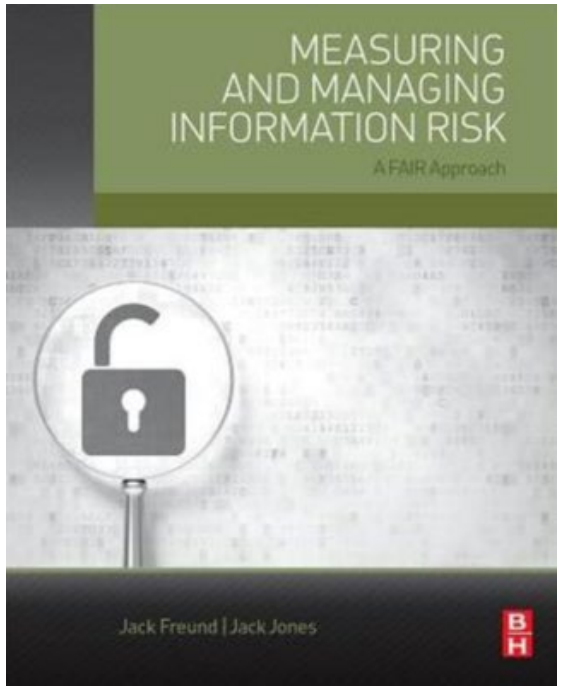
CYBERSECURITY
CANON

https://cybercanon.paloaltonetworks.com/

Why this Talk?

Jack Jones

Jack Freund



https://cybercanon.paloaltonetworks.com/award-winners/

CYBERSECURITY
CANON
paloalto NETWORKS

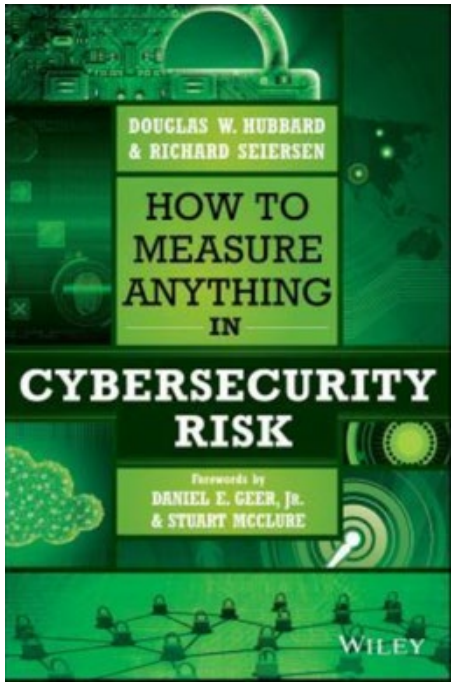
https://cybercanon.paloaltonetworks.com/

paloalto NETWORKS

Why this Talk?

Douglas Hubbard

Richard Seirsen



CYBERSECURITY
CANON

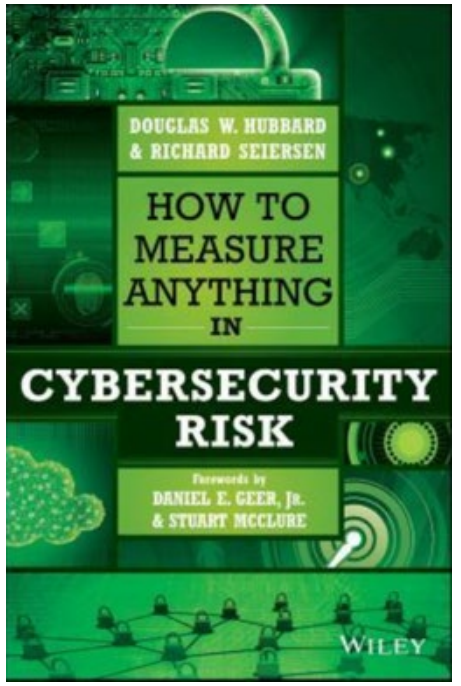
https://cybercanon.paloaltonetworks.com/

Why this Talk?

https://cybercanon.paloaltonetworks.com/award-winners/

Douglas Hubbard

Richard Seirsen



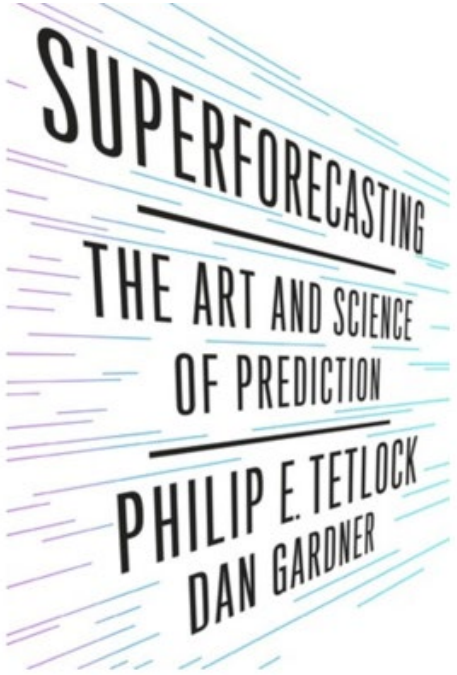
CYBERSECURITY CANON

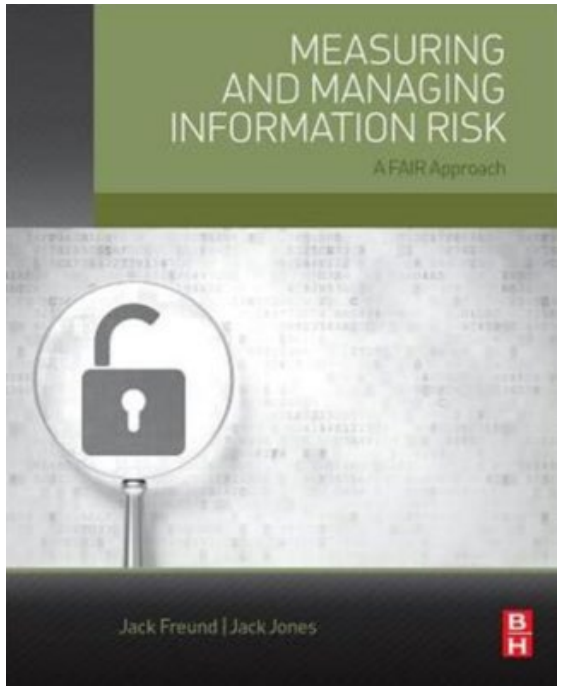
https://cybercanon.paloaltonetworks.com/

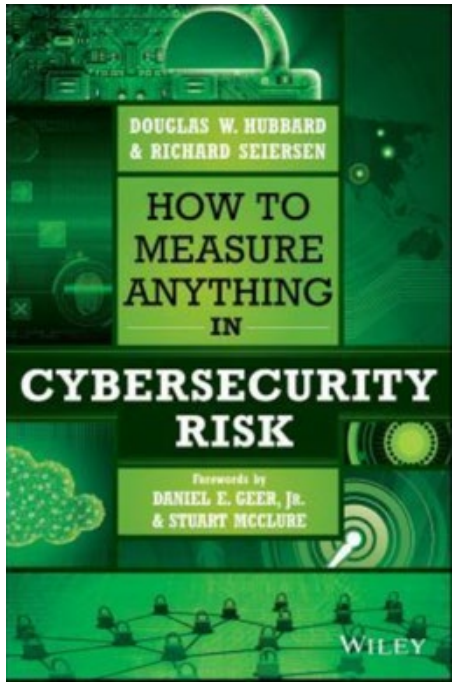
paloalto NETWORKS

RSAConference2019

Why this Talk?







CYBERSECURITY
CANON

https://cybercanon.paloaltonetworks.com/

Transition

RSAConference2019

Heat Maps are Bad Science

Heat Maps are Bad Science

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Typical Risk Register

Risk	Description
1	Loss of customer records
2	Zero day found in primary code that gives root access
3	Spear phishing gains access to CEO
4	Catastrophic power failure of main facility taking it offline > 72 hours
…	
N	Godzilla crushes company data center

Heat Maps are Bad Science

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Heat Maps are Poor Vehicles for Conveying Risk

2005: Surveyed NATO Officers believe that Highly Likely could mean anywhere between 40% and 100% likely. - Heuer

2006: Studies find that experts choose "1" more often in a scale of say "1" to "10" regardless of the subject matter the number is supposed to represent. - Rottenstreich

2008: Ordinal scales inadvertently create range compression; a kind of extreme rounding error. - Cox

2009: Surveyed students and faculty believe that “Very Likely” could mean anywhere between 43% and 99% likely. - Budescu

2016: Cybersecurity scoring systems like OWASP (Open Web Access Security Project), CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the CCSS (Common Configuration Scoring System) perform improper math on non-mathematical objects to aggregate a risk score. - Hubbard/Seirsen

2016: The idea of “Risk Tolerance” is not presented. Just because risk officers rate an event as highly likely does not mean that leadership is not willing to accept that risk. - Hubbard/Seirsen

2016: Heat maps convey no information about when the event might happen (next year, next three years, next decade.) - Hubbard/Seirsen

2016: Some risk officers rate events as more likely just because they could be more impactful. - Hubbard/Seirsen

2016: When percentages were explicitly defined, highly likely is between 90% and 99% for example, survey participants violated the rules over half the time. - Hubbard/Seirsen

2016: Most surveyed experts using ordinal scales from "1" to "5" chose the values of "3" or "4" reducing the 5X5 matrix to a 2X2 matrix. - Hubbard/Seirsen

Heat Maps are Bad Science

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Heat Maps are Poor Vehicles for Conveying Risk

2005: Surveyed NATO Officers believe that Highly Likely could mean anywhere between 40% and 100% likely. - Heuer

2006: Studies find that experts choose "1" more often in a scale of say "1" to "10" regardless of the subject matter the number is supposed to represent. - Rottenstreich

2008: Ordinal scales inadvertently create range compression; a kind of extreme rounding error. - Cox

2009: Surveyed students and faculty believe that "Very Likely" could mean anywhere between 43% and 99% likely. - Budescu

2016: Cybersecurity scoring systems like OWASP (Open Web Access Security Project), CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the CCSS (Common Configuration Scoring System) perform improper math on non-mathematical objects to aggregate a risk score. - Hubbard/Seirsen

2016: The idea of "Risk Tolerance" is not presented. Just because risk officers rate an event as highly likely does not mean that leadership is not willing to accept that risk. - Hubbard/Seirsen

2016: Heat maps convey no information about when the event might happen (next year, next three years, next decade.) - Hubbard/Seirsen

2016: Some risk officers rate events as more likely just because they could be more impactful. - Hubbard/Seirsen

2016: When percentages were explicitly defined, highly likely is between 90% and 99% for example, survey participants violated the rules over half the time. - Hubbard/Seirsen

2016: Most surveyed experts using ordinal scales from "1" to "5" chose the values of "3" or "4" reducing the 5X5 matrix to a 2X2 matrix. - Hubbard/Seirsen

Heat Maps are Bad Science

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Heat Maps are Poor Vehicles for Conveying Risk

2005: Surveyed NATO Officers believe that Highly Likely could mean anywhere between 40% and 100% likely. - Heuer

2006: Studies find that experts choose "1" more often in a scale of say "1" to "10" regardless of the subject matter the number is supposed to represent. - Rottenstreich

2008: Ordinal scales inadvertently create range compression; a kind of extreme rounding error. - Cox

2009: Surveyed students and faculty believe that "Very Likely" could mean anywhere between 43% and 99% likely. - Budescu

2016: Cybersecurity scoring systems like OWASP (Open Web Access Security Project), CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the CCSS (Common Configuration Scoring System) perform improper math on non-mathematical objects to aggregate a risk score. - Hubbard/Seirsen

2016: The idea of "Risk Tolerance" is not presented. Just because risk officers rate an event as highly likely does not mean that leadership is not willing to accept that risk. - Hubbard/Seirsen

2016: Heat maps convey no information about when the event might happen (next year, next three years, next decade.) - Hubbard/Seirsen

2016: Some risk officers rate events as more likely just because they could be more impactful. - Hubbard/Seirsen

2016: When percentages were explicitly defined, highly likely is between 90% and 99% for example, survey participants violated the rules over half the time. - Hubbard/Seirsen

2016: Most surveyed experts using ordinal scales from "1" to "5" chose the values of "3" or "4" reducing the 5X5 matrix to a 2X2 matrix. - Hubbard/Seirsen

Heat Maps are Bad Science

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Heat Maps are Poor Vehicles for Conveying Risk

2005: Surveyed NATO Officers believe that Highly Likely could mean anywhere between 40% and 100% likely. - Heuer

2006: Studies find that experts choose "1" more often in a scale of say "1" to "10" regardless of the subject matter the number is supposed to represent. - Rottenstreich

2008: Ordinal scales inadvertently create range compression; a kind of extreme rounding error. - Cox

2009: Surveyed students and faculty believe that "Very Likely" could mean anywhere between 43% and 99% likely. - Budescu

2016: Cybersecurity scoring systems like OWASP (Open Web Access Security Project), CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the CCSS (Common Configuration Scoring System) perform improper math on non-mathematical objects to aggregate a risk score. - Hubbard/Seirsen

2016: The idea of "Risk Tolerance" is not presented. Just because risk officers rate an event as highly likely does not mean that leadership is not willing to accept that risk. - Hubbard/Seirsen

2016: Heat maps convey no information about when the event might happen (next year, next three years, next decade.) - Hubbard/Seirsen

2016: Some risk officers rate events as more likely just because they could be more impactful. - Hubbard/Seirsen

2016: When percentages were explicitly defined, highly likely is between 90% and 99% for example, survey participants violated the rules over half the time. - Hubbard/Seirsen

2016: Most surveyed experts using ordinal scales from "1" to "5" chose the values of "3" or "4" reducing the 5X5 matrix to a 2X2 matrix. - Hubbard/Seirsen

paloalto NETWORKS

Transition

RSAConference2019

What CISOs know about Probability is Likely Wrong

You are Doing it Wrong!

Professor
Ronald
Howard

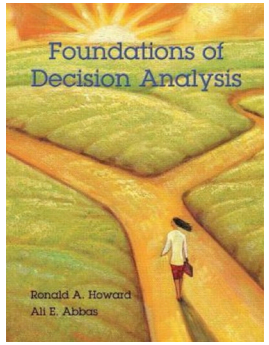
You are Doing it Wrong!

Professor
Ronald
Howard

Bio

Ronald A. Howard has been Professor in the Department of Engineering-Economic Systems (now the Department of Management Science and Engineering) in the School of Engineering of Stanford University since 1965. Professor Howard is one of the founders of the decision analysis discipline. His books on probabilistic modeling, decision analysis, dynamic programming, and Markov processes serve as major references for courses and research in these fields.

You are Doing it Wrong!

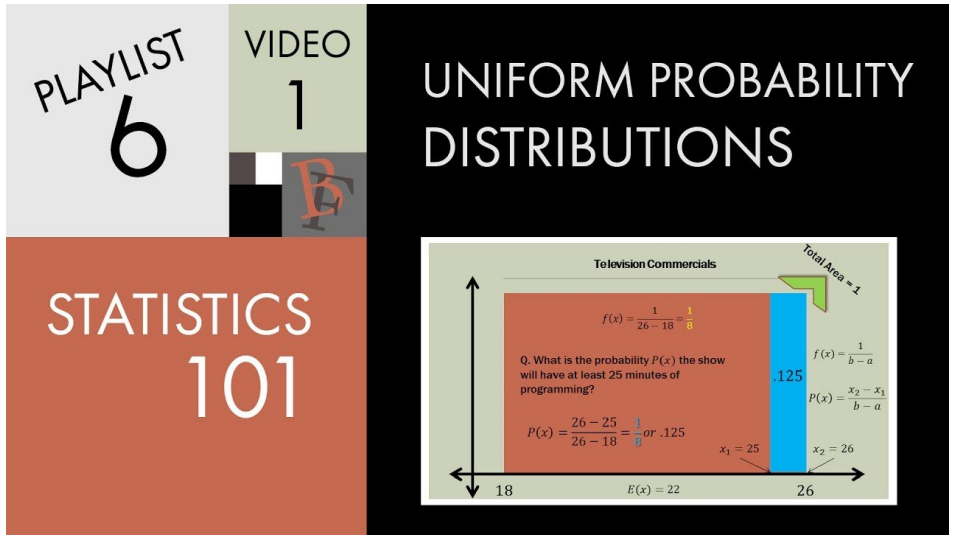


Professor Ronald Howard

Bio

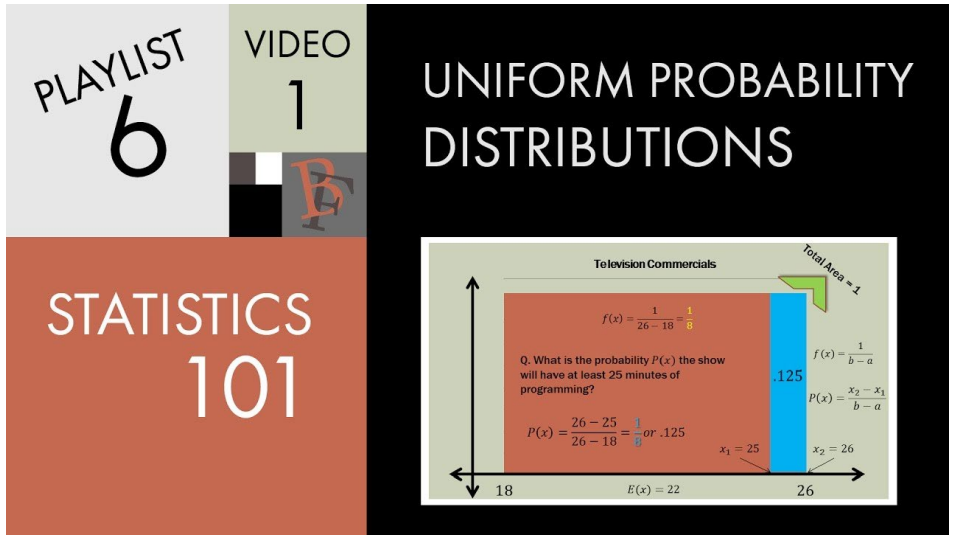
Ronald A. Howard has been Professor in the Department of Engineering-Economic Systems (now the Department of Management Science and Engineering) in the School of Engineering of Stanford University since 1965. Professor Howard is one of the founders of the decision analysis discipline. His books on probabilistic modeling, decision analysis, dynamic programming, and Markov processes serve as major references for courses and research in these fields.

You are Doing it Wrong!



Professor Ronald Howard

You are Doing it Wrong!



Professor Ronald Howard

Calculating probability

boardworks

If the outcomes of an event are equally likely then we can calculate the probability using the formula:

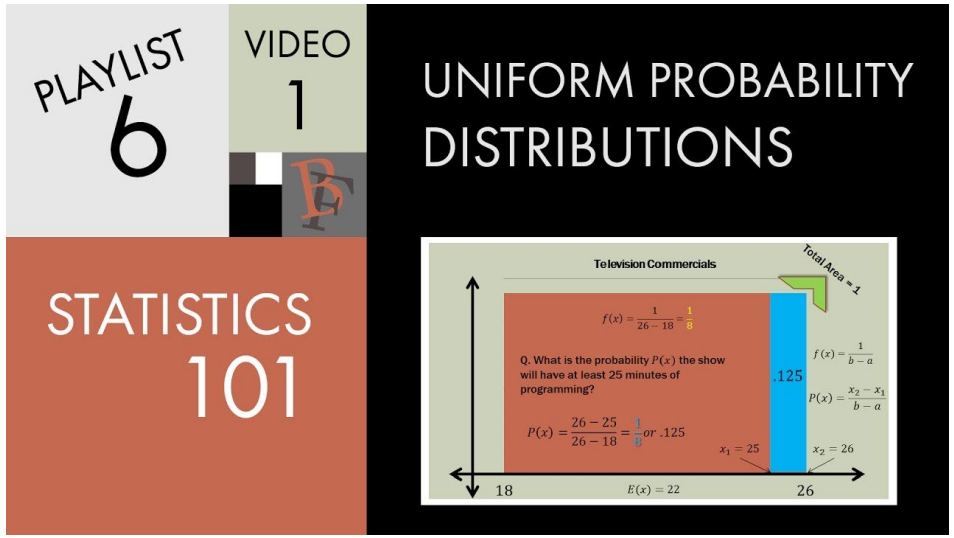
$$\text{Probability of an event} = \frac{\text{Number of successful outcomes}}{\text{Total number of possible outcomes}}$$

For example, a bag contains 1 yellow, 3 green, 4 blue and 2 red marbles.

What is the probability of pulling a green marble from the bag without looking?

$P(\text{green}) = \frac{3}{10}$ or 0.3 or 30%

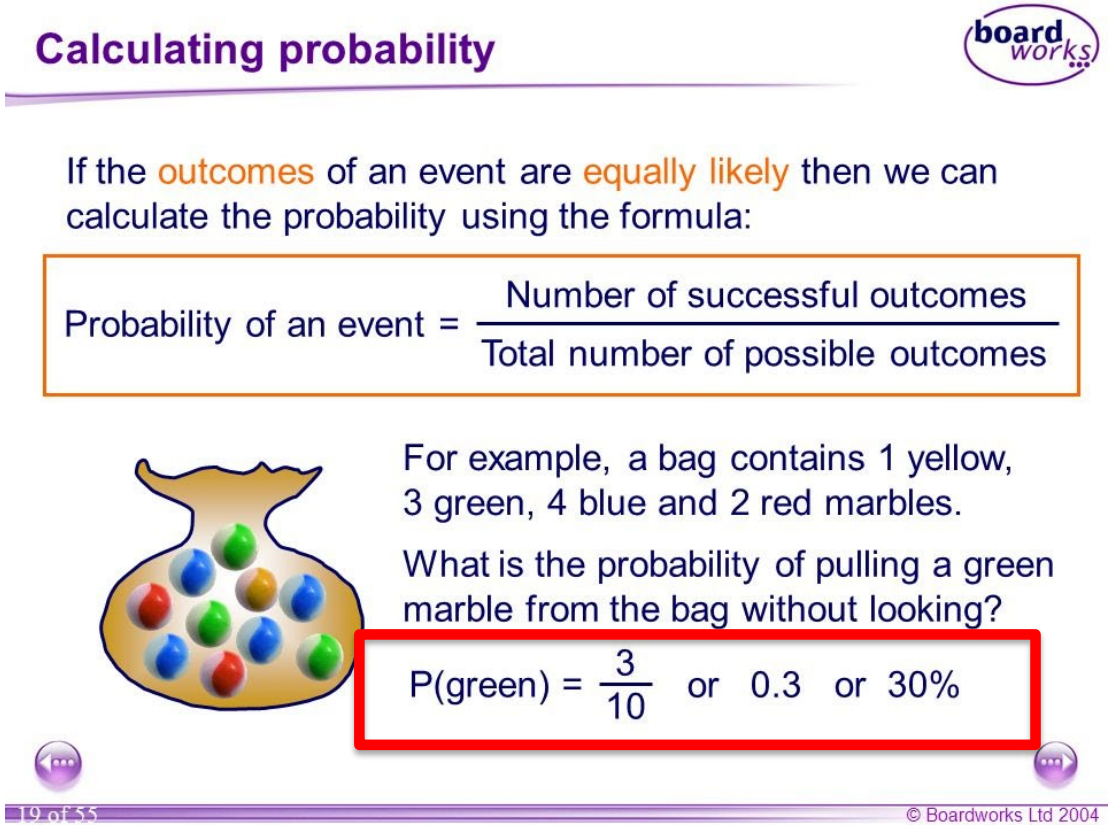
You are Doing it Wrong!



Professor Ronald Howard

Typical CISO:

"Probabilities can be found in the data."



You are Doing it Wrong!

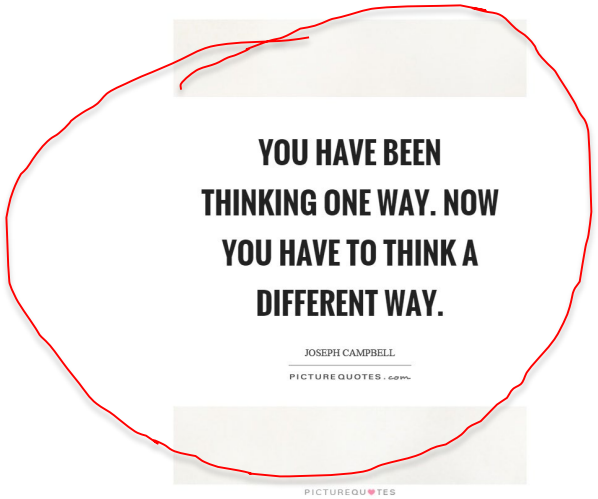
Professor Ronald Howard

"Only a person can assign a probability, taking into account any data or other knowledge available."

You are Doing it Wrong!

Professor Ronald Howard

"Only a person can assign a probability, taking into account any data or other knowledge available."



For example, a bag contains 1 yellow, 3 green, 4 blue and 2 red marbles.

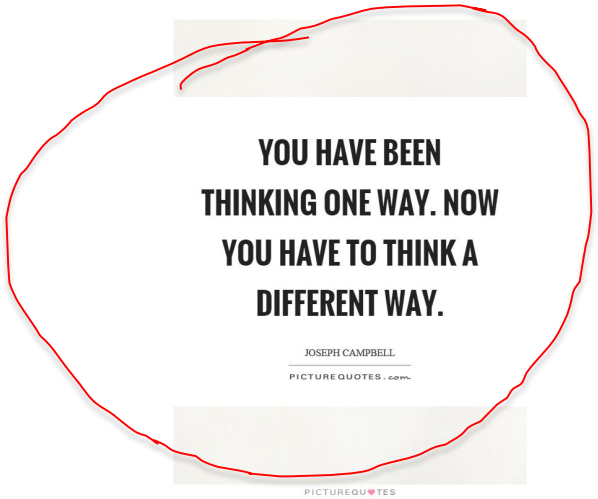
What is the probability of pulling a green marble from the bag without looking?

$P(\text{green}) = \frac{3}{10}$ or 0.3 or 30%

You are Doing it Wrong!

Professor Ronald Howard

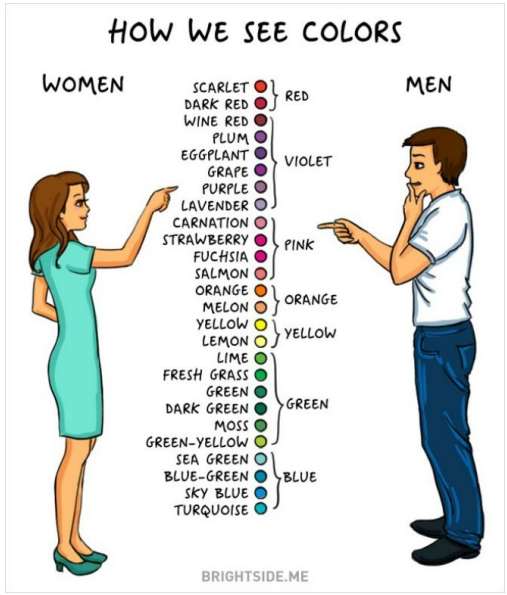
"A probability reflects a person's knowledge (or equivalently ignorance) about some uncertain distinction."



You are Doing it Wrong!

Professor Ronald Howard

"A probability reflects a person's knowledge (or equivalently ignorance) about some uncertain distinction."



Nuance

You are Doing it Wrong!

Professor Ronald Howard

"A probability reflects a person's knowledge (or equivalently ignorance) about some uncertain distinction."

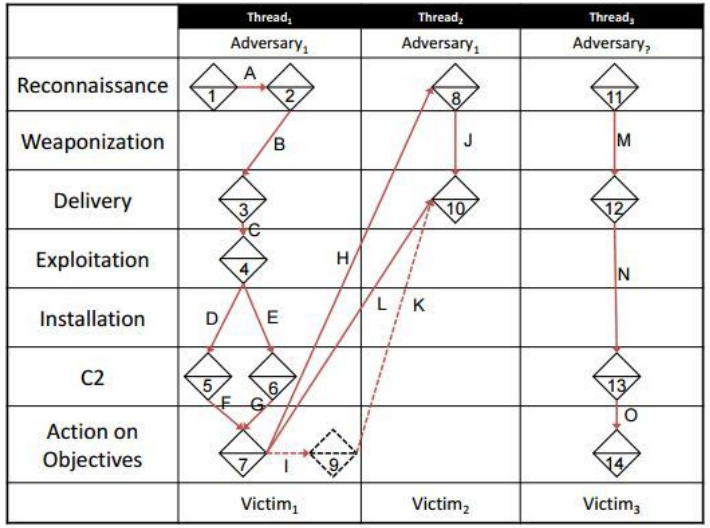
Better Risk Register

Risk	Description	Probability
1	What is the probability that a loss of customer records due to a cyber event in the next three years will materially impact the organization?	5% – 12%
2	What is the probability that a Zero day found in primary code that allows root access in the next three years will materially impact the organization?	1% - 3%
3	What is the probability that a Spear phishing attack that exposes the CEO in the next three years will materially impact the organization?	7% - 15%
4	What is the probability that a catastrophic power failure in the next three years that takes the company offline for > 72 hours will materially impact the organization?	1% - 2%
...		
N	What is the probability that Godzilla crushes the company data center in the next three years and will materially impact the organization?	80% - 90%

You are Doing it Wrong!

Professor Ronald Howard

"A probability reflects a person's knowledge (or equivalently ignorance) about some uncertain distinction."



For example, a bag contains 1 yellow, 3 green, 4 blue and 2 red marbles.

What is the probability of pulling a green marble from the bag without looking?

$P(\text{green}) = \frac{3}{10}$ or 0.3 or 30%

You are Doing it Wrong!

Information – what you know

Alternatives – what you can do

Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

Information – what you know

Alternatives – what you can do

Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

Information – what you know

Alternatives – what you can do

Professor Ronald Howard

Preferences – what you want

You are Doing it Wrong!

Information – what you know

Alternatives – what you can do

Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

Professor Ronald Howard

All Information

- Information – what you know
- Alternatives – what you can do
- Preferences – what you want

You are Doing it Wrong!

Professor Ronald Howard

All Information

- Information – what you know
- Alternatives – what you can do
- Preferences – what you want

You are Doing it Wrong!

I KNOW ABSOLUTELY

All Information

- Information – what you know
- Alternatives – what you can do
- Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

I KNOW ABSOLUTELY

I HAVE NO IDEA

All Information

Information – what you know

Alternatives – what you can do

Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

I KNOW ABSOLUTELY

I HAVE NO IDEA

I HAVE A GUESS, AN ESTIMATE

All Information

Information – what you know

Alternatives – what you can do

Preferences – what you want

Professor Ronald Howard

You are Doing it Wrong!

I KNOW ABSOLUTELY

I HAVE A GUESS

All Information

Alternatives – what you can do

Professor Ronald Howard

You are Doing it Wrong!

I KNOW ABSOLUTELY

I

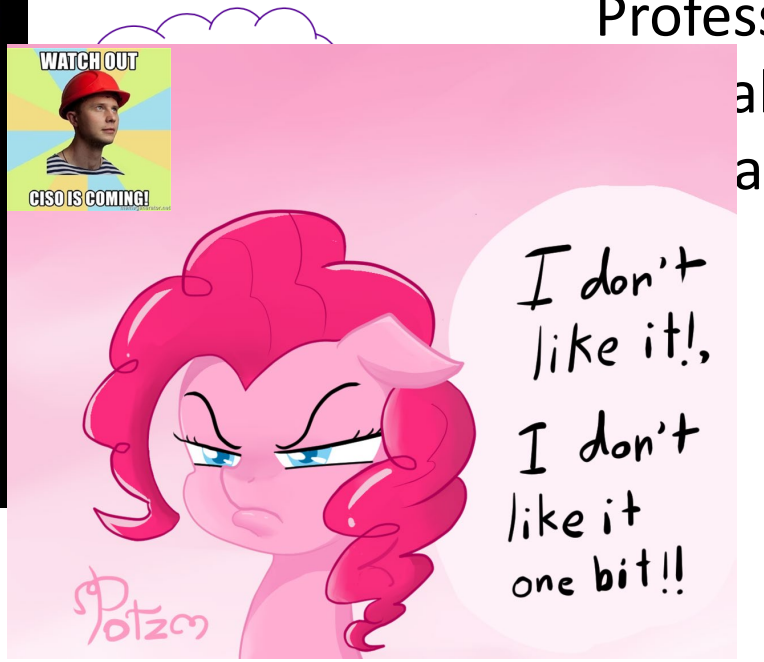
I HAVE A GUESS

All Information

Professor

ald

ard



You are Doing it Wrong!

"Don't think of **probability** or uncertainties as the **lack of knowledge**.

Professor Ronald Howard

You are Doing it Wrong!

Professor Ronald Howard

"Don't think of **probability** or uncertainties as the lack of knowledge. Think of them instead as a very detailed **description of exactly what you know**."

You are Doing it Wrong!

Professor Ronald Howard

"Don't think of **probability** or uncertainties as the lack of knowledge. Think of them instead as a very detailed **description of exactly what you know**."

Transition

RSAConference2019

Bayes and Monte Carlo History

History of Bayesian Measurement

Source: University of York, 2013

1740s

History of Bayesian Measurement

1740s

Likelihood

How probable is the evidence given that our hypothesis is true?

Prior

How probable was our hypothesis before observing the evidence?

$$P(H \mid e) = \frac{P(e \mid H)\, P(H)}{P(e)}$$

Posterior

How probable is our hypothesis given the observed evidence?

Marginal

How probable is new evidence under all possible hypotheses?

History of Bayesian Measurement


Source: University of York, 2013

1740s

Likelihood

How probable is the evidence given that our hypothesis is true?

Prior

How probable was our hypothesis before observing the evidence?

$$P(H \mid e) = \frac{P(e \mid H)\, P(H)}{P(e)}$$

Posterior

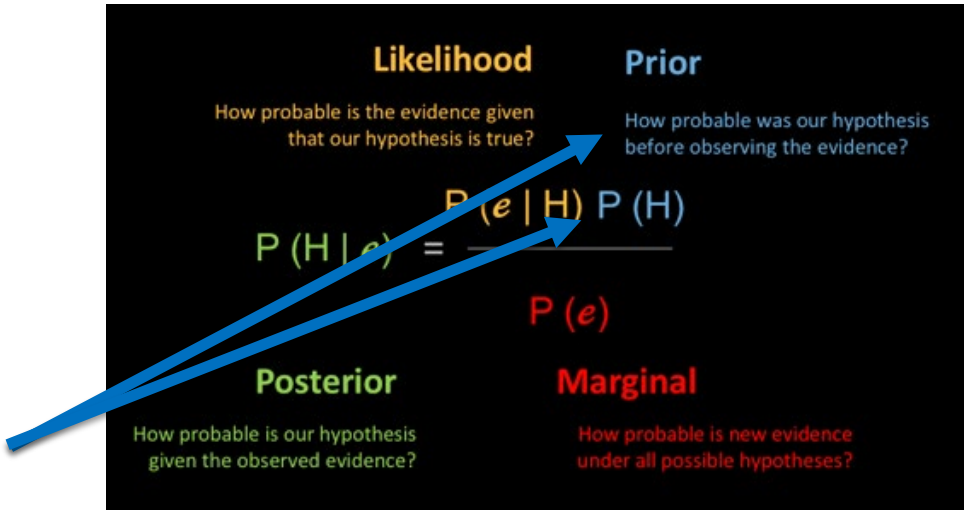
How probable is our hypothesis given the observed evidence?

Marginal

How probable is new evidence under all possible hypotheses?

History of Bayesian Measurement

1740s



History of Bayesian Measurement


Source: University of York, 2013

1740s

Likelihood

How probable is the evidence given that our hypothesis is true?

Prior

How probable was our hypothesis before observing the evidence?

$$P(H \mid e) = \frac{P(e \mid H)\, P(H)}{P(e)}$$

Posterior

How probable is our hypothesis given the observed evidence?

Marginal

How probable is new evidence under all possible hypotheses?

History of Bayesian Measurement


Source: University of York, 2013

1740s

Likelihood

How probable is the evidence given that our hypothesis is true?

Prior

How probable was our hypothesis before observing the evidence?

$$P(H \mid e) = \frac{P(e \mid H)\, P(H)}{P(e)}$$

Posterior

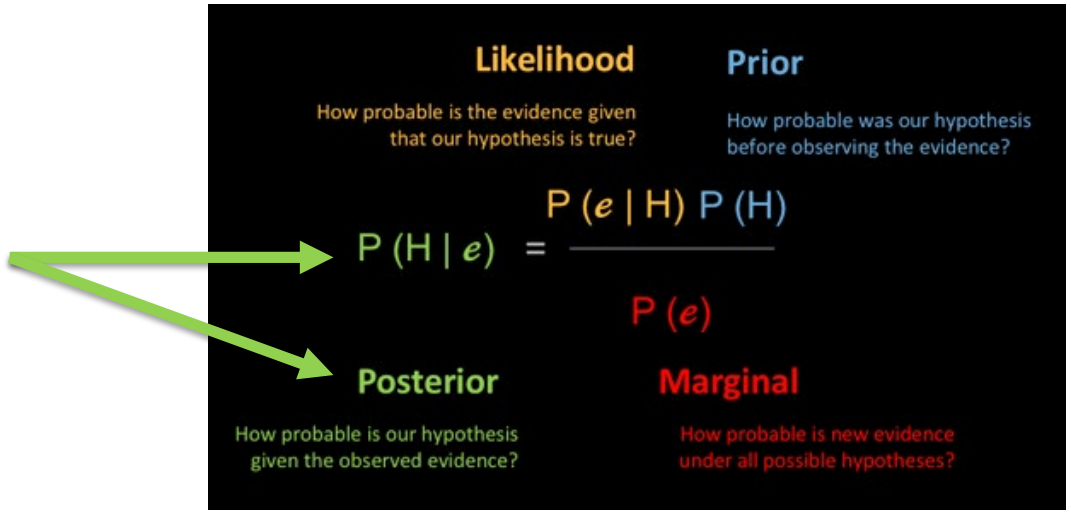
How probable is our hypothesis given the observed evidence?

Marginal

How probable is new evidence under all possible hypotheses?

History of Bayesian Measurement

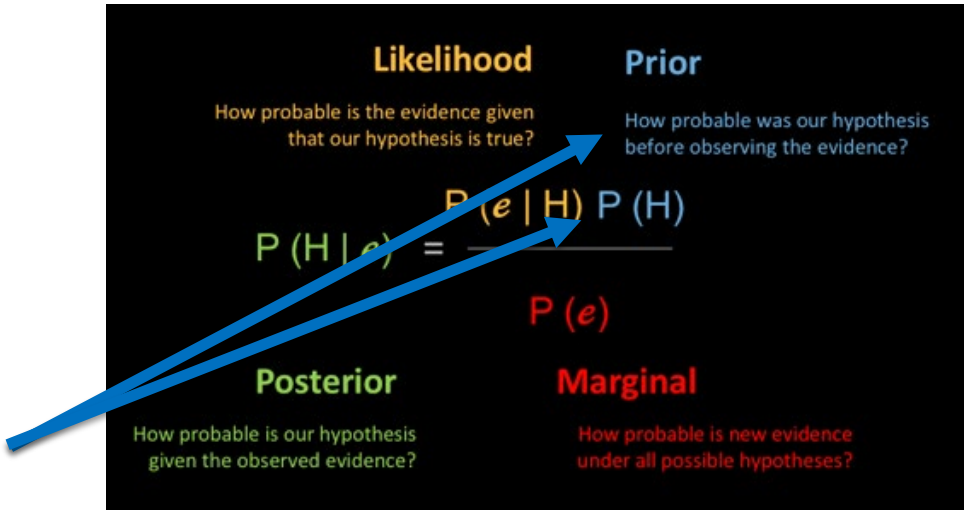
1740s



What is the Probability of a material breach in the next three years?

History of Bayesian Measurement

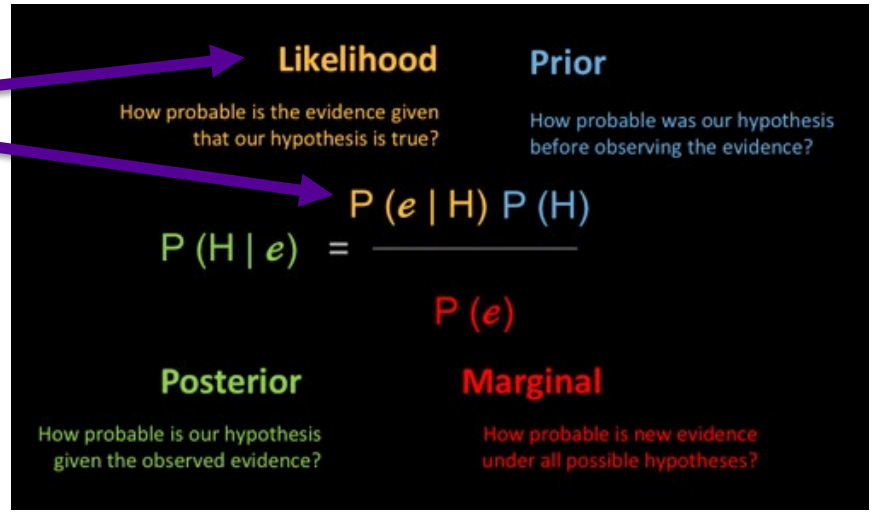
1740s



What is the Probability of a material breach in the next three years?

History of Bayesian Measurement

1740s



What is the Probability of a material breach in the next three years?

History of Bayesian Measurement

Do Not Freak Out

Likelihood

How probable is the evidence given that our hypothesis is true?

Prior

How probable was our hypothesis before observing the evidence?

$$P(H \mid e) = \frac{P(e \mid H)\, P(H)}{P(e)}$$

Posterior

e is our hypothesis
bserved evidence?

Marginal

How probable is new evidence under all possible hypotheses?

History of Bayesian Measurement

Source: University of York, 2013

History of Bayesian Measurement

Source: University of York, 2013

Frequentists Viewpoint

History of Bayesian Measurement

Source: University of York, 2013

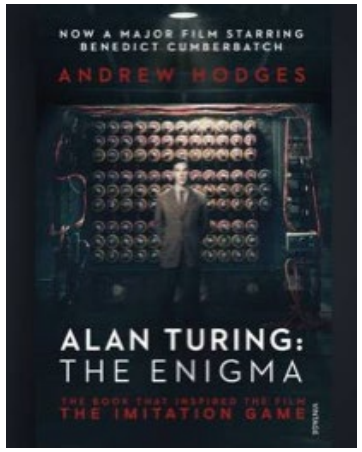
Complex Problems

Frequentists Viewpoint

PERMANENT LINK TO THIS COMIC: HTTPS://XKCD.COM/795/
IMAGE URL (FOR HOTLINKING/EMBEDDING): HTTPS://IMGS.XKCD.COM/COMICS/CONDITIONAL_RISK.PNG

History of Bayesian Measurement

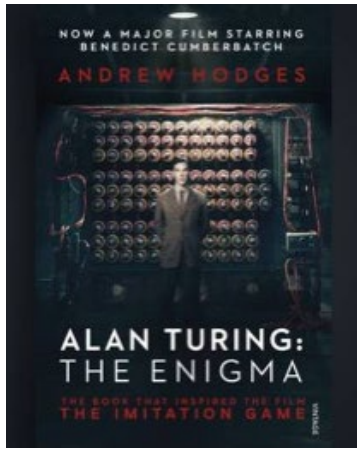
Source: University of York, 2013



Frequentists Viewpoint

History of Bayesian Measurement

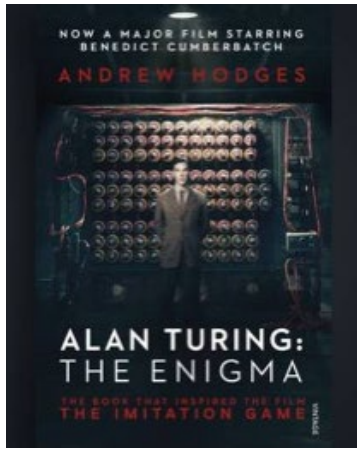
Source: University of York, 2013



Frequentists Viewpoint

History of Bayesian Measurement


Source: University of York, 2013

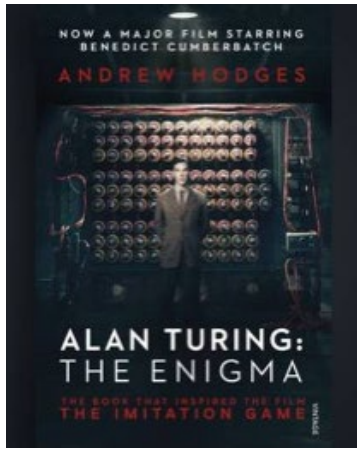



Stanislaw Ulam, John von Neumann, and Nicholas Metropolis

Frequentists Viewpoint

History of Bayesian Measurement


Source: University of York, 2013




Stanislaw Ulam, John von Neumann, and Nicholas Metropolis

Frequentists Viewpoint

History of Bayesian Measurement

Source: University of York, 2013

Frequentists Viewpoint

Transition

RSAConference2019

How to Think about Superforecasting

How to Think about Superforecasting

What is the likelihood that a certain cyber event will happen?

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

“Cyber”

Misrepresent Risk

How to Think about Superforecasting

What is the likelihood that a certain cyber event will happen?

NO

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

“Cyber”

Misrepresent Risk

How to Think about Superforecasting

What is the likelihood that a certain cyber event will happen?

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

Misrepresent Risk

NO

"Cyber"

YES

paloalto NETWORKS

How to Think about Superforecasting

“Cyber”

How to Think about Superforecasting

Force Multiplier

"Cyber"

How to Think about Superforecasting

- CYBER **ESPIONAGE**
- CYBER **CRIME**
- CYBER **HACKTIVISM**
- CYBER **WARFARE**
- CYBER **MISCHIEF**
- CYBER **TERRORISM**
- **INFORMATION OPS**

"Cyber"

YES

paloalto NETWORKS

How to Think about Superforecasting

- CYBER **ESPIONAGE**
- CYBER **CRIME**
- CYBER **HACKTIVISM**
- CYBER **WARFARE**
- CYBER **MISCHIEF**
- CYBER **TERRORISM**
- **INFORMATION OPS**

“Cyber Risk”

needs more Precision

paloalto NETWORKS

How to Think about Superforecasting

How to Think about Superforecasting

What is the likelihood that a certain cyber event will happen?

How to Think about Superforecasting

What is the Probability of a material breach in the next three years?

~~What is the likelihood that a certain cyber event will happen?~~

How to Think about Superforecasting

~~What is the likelihood that a certain cyber event will happen?~~

What is the Probability of a material breach in the next three years?

I am confident that within the next three years, the probability of a material impact to the company due to a computer breach is between 2% and 12%.

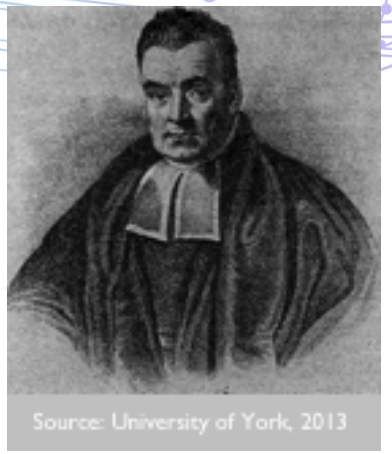
How to Think about Superforecasting

~~What is the **likelihood** that a certain cyber event will happen?~~

What is the **Probability** of a material breach in the next three years?

I am confident that within the next three years, the **probability** of a material impact to the company due to a computer breach is between 2% and 12%.

How to Think about Superforecasting



What is the **Probability** of a material breach in the next three years?

~~What is the **likelihood** that a certain cyber event will happen?~~

I am confident that within the next three years, the **probability** of a material impact to the company due to a computer breach is between 2% and 12%.

paloalto NETWORKS

How to Think about Superforecasting

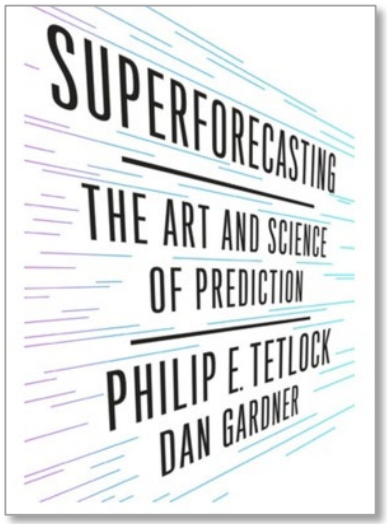
~~What is the likelihood that a certain cyber event will happen?~~

What is the Probability of a material breach **in the next three years**?

I am confident that **within the next three years**, the probability of a material impact to the company due to a computer breach is between 2% and 12%.

How to Think about Superforecasting

~~What is the likelihood that a certain cyber event will happen?~~



What is the Probability of a material breach in the next three years?

I am confident that within the next three years, the probability of a material impact to the company due to a computer breach is **between 2% and 12%**.

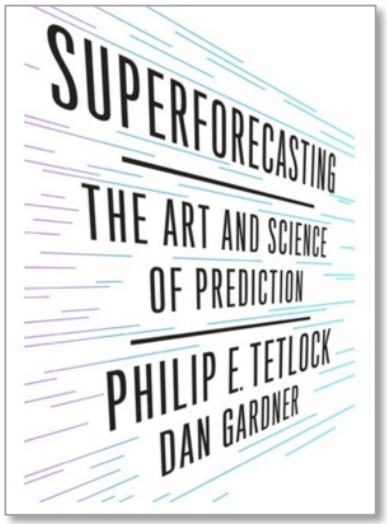
How to Think about Superforecasting

More Precise than this

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

~~What is the likelihood that a certain cyber event will happen?~~

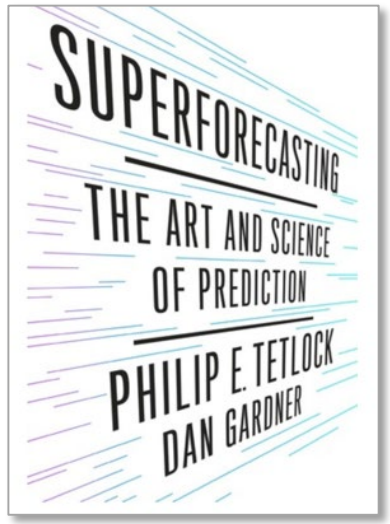
What is the Probability of a material breach in the next three years?



I am confident that within the next three years, the probability of a material impact to the company due to a computer breach is **between 2% and 12%**.

How to Think about Superforecasting

The $1000 Bet

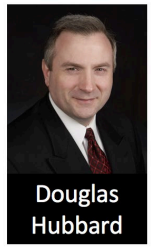


What is the Probability of a material breach in the next three years?

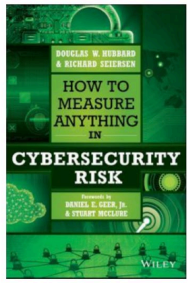
I am confident that within the next three years, the probability of a material impact to the company due to a computer breach is **between 2% and 12%**.

How to Think about Superforecasting

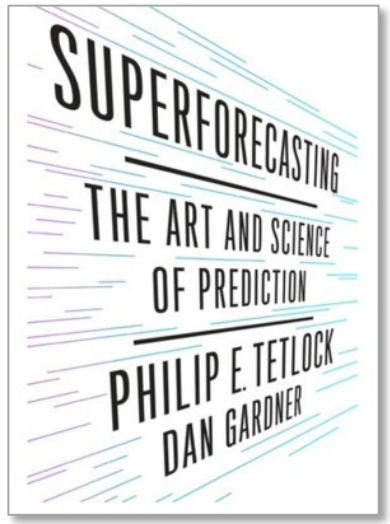
The $1000 Bet


Douglas Hubbard


Richard Seirsen



CYBERSECURITY CANON
https://cybercanon.paloaltonetworks.com/



What is the Probability of a material breach in the next three years?

I am confident that within the next three years, the probability of a material impact to the company due to a computer breach is **between 2% and 12%**.

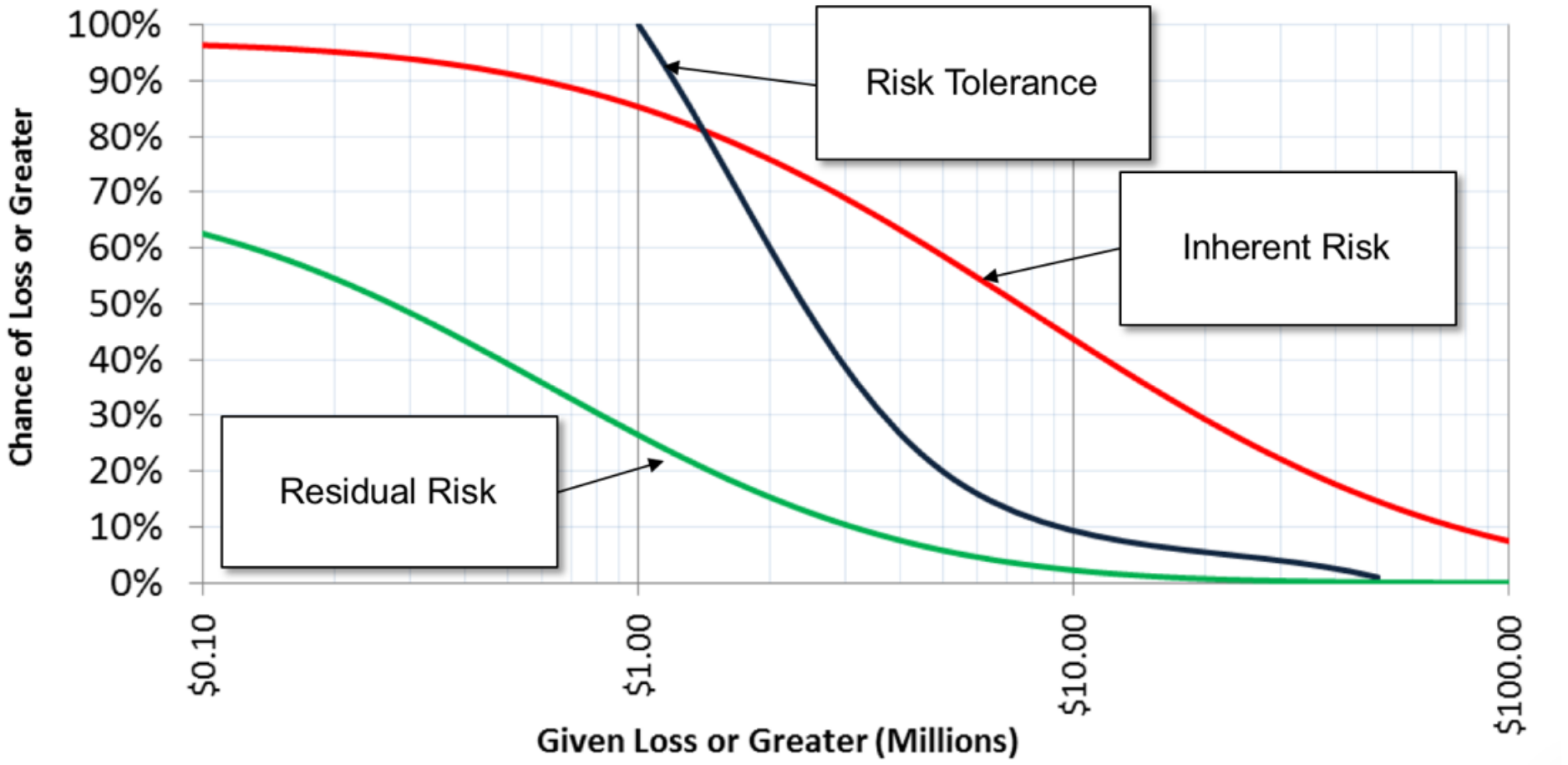
paloalto NETWORKS

Transition

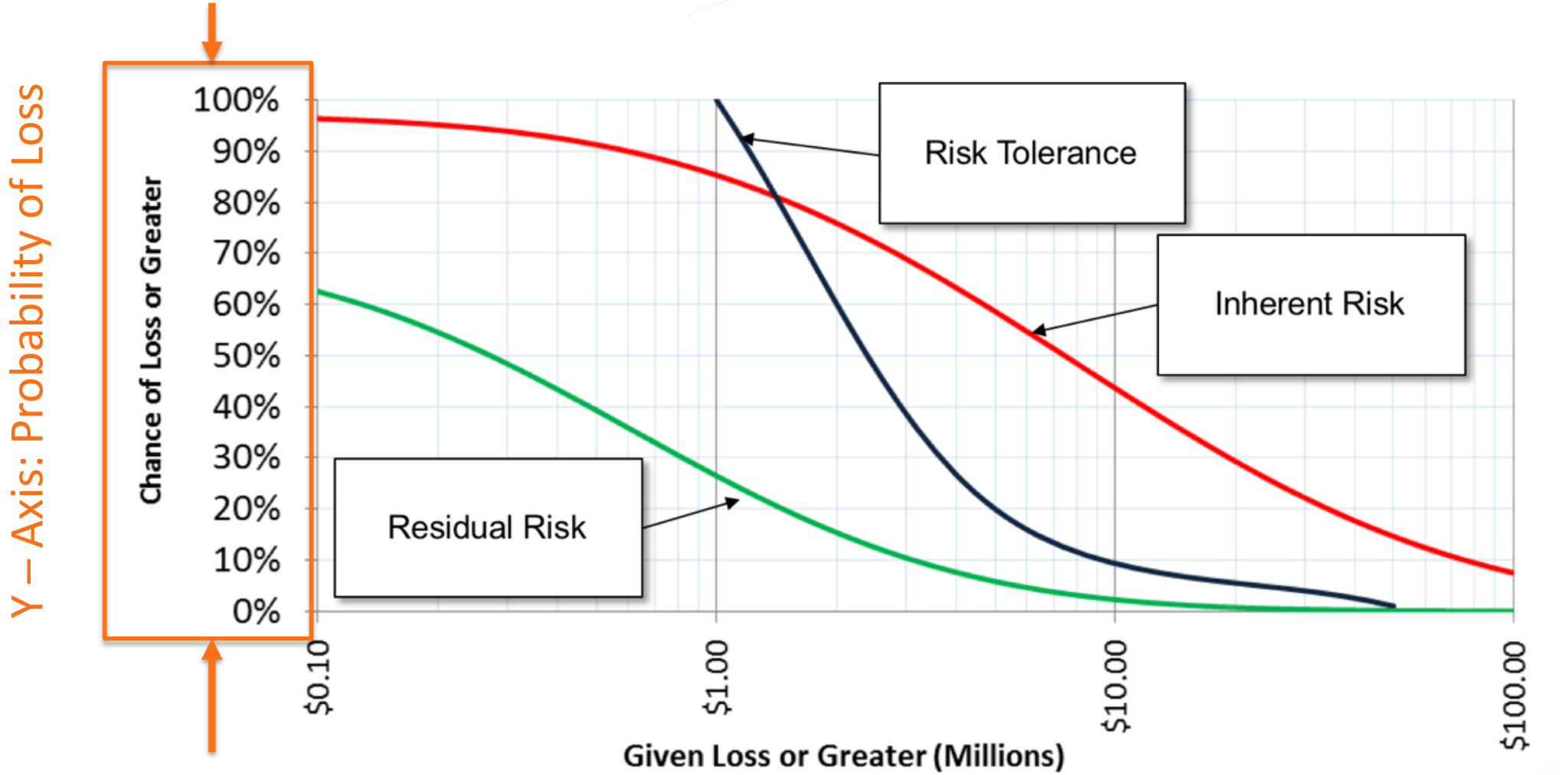
RSAConference2019

Replace Heat Maps with Latency Curves

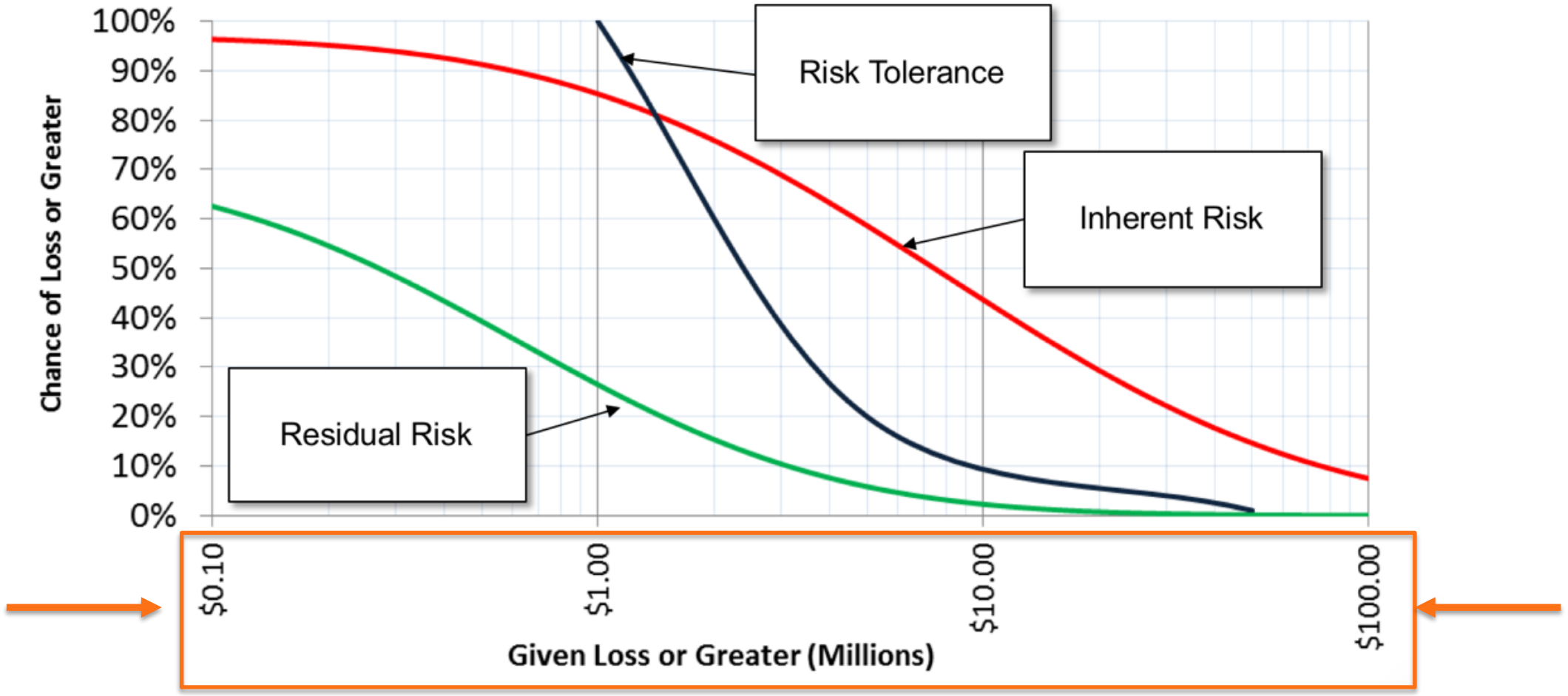
Loss Exceedance Curves



Loss Exceedance Curves

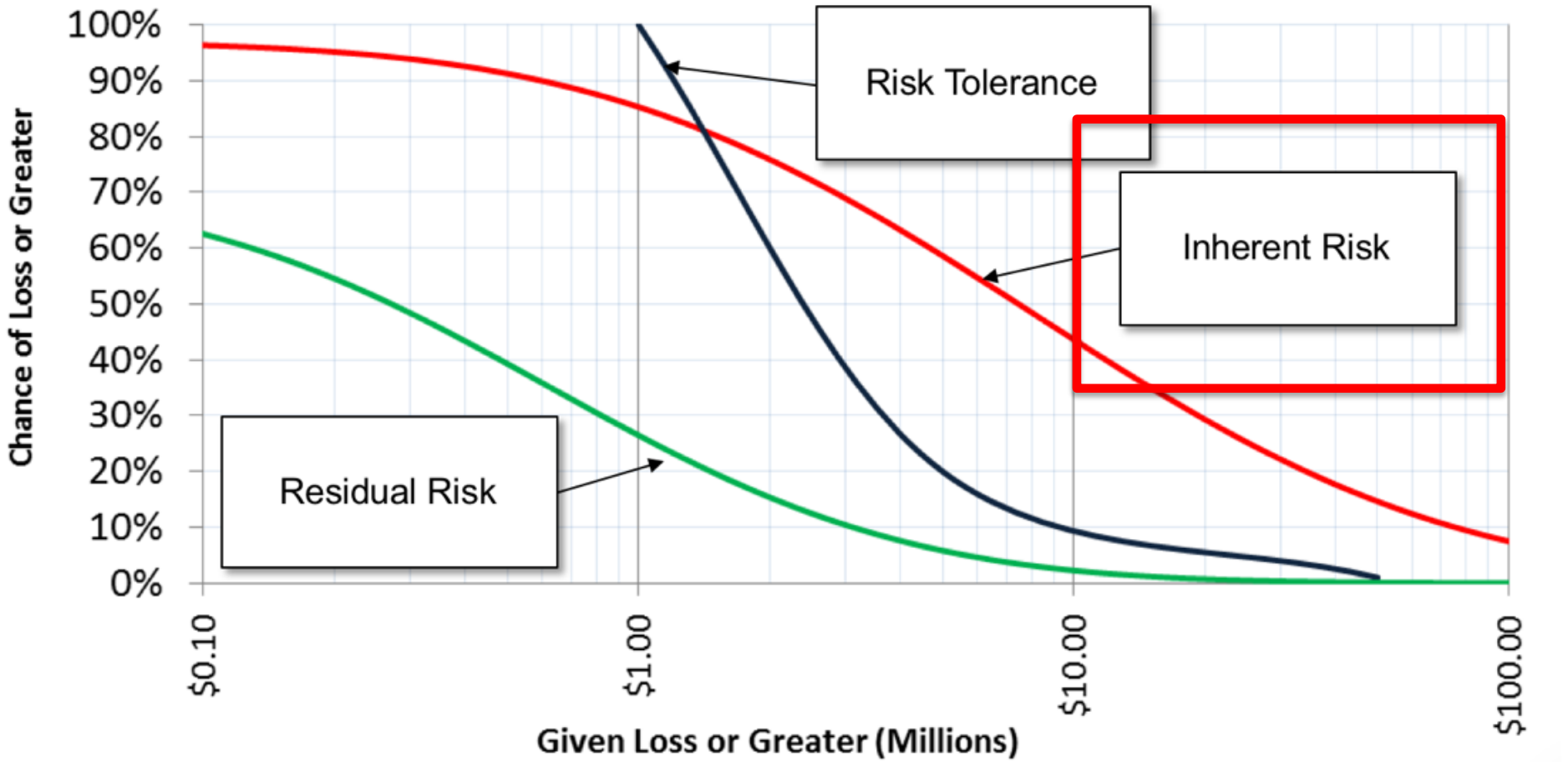


Loss Exceedance Curves



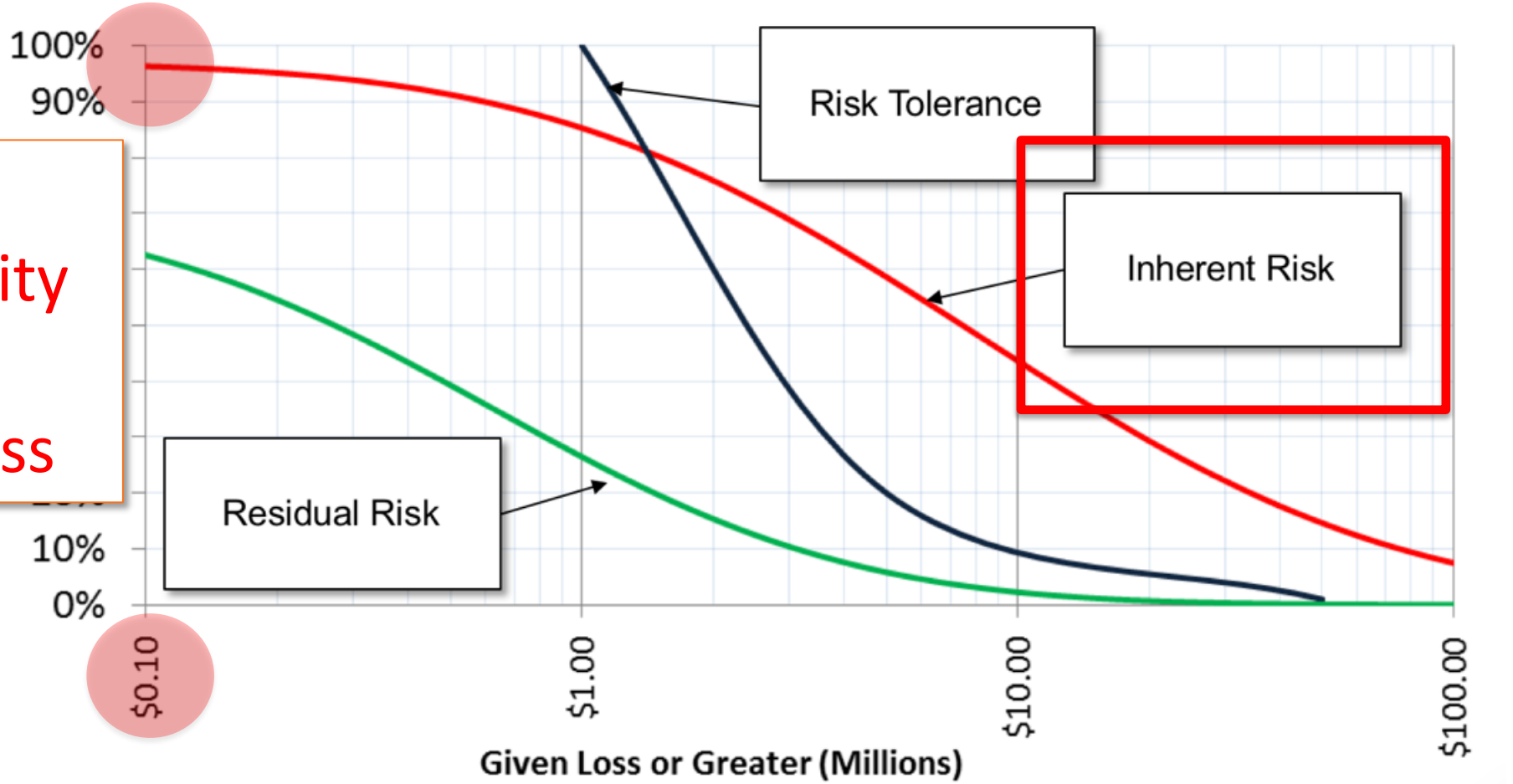
X – Axis: Estimate of Loss

Loss Exceedance Curves

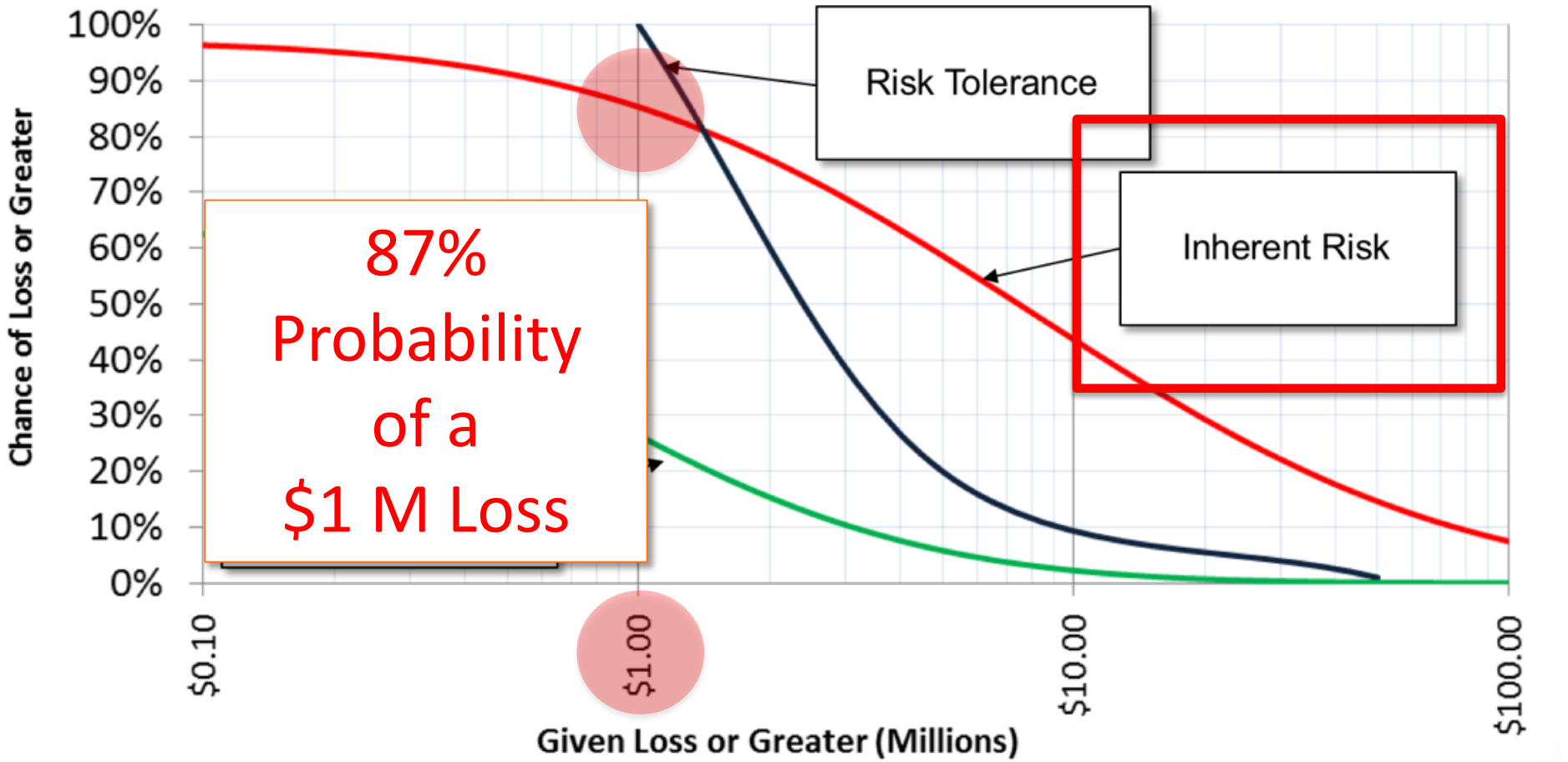


Loss Exceedance Curves

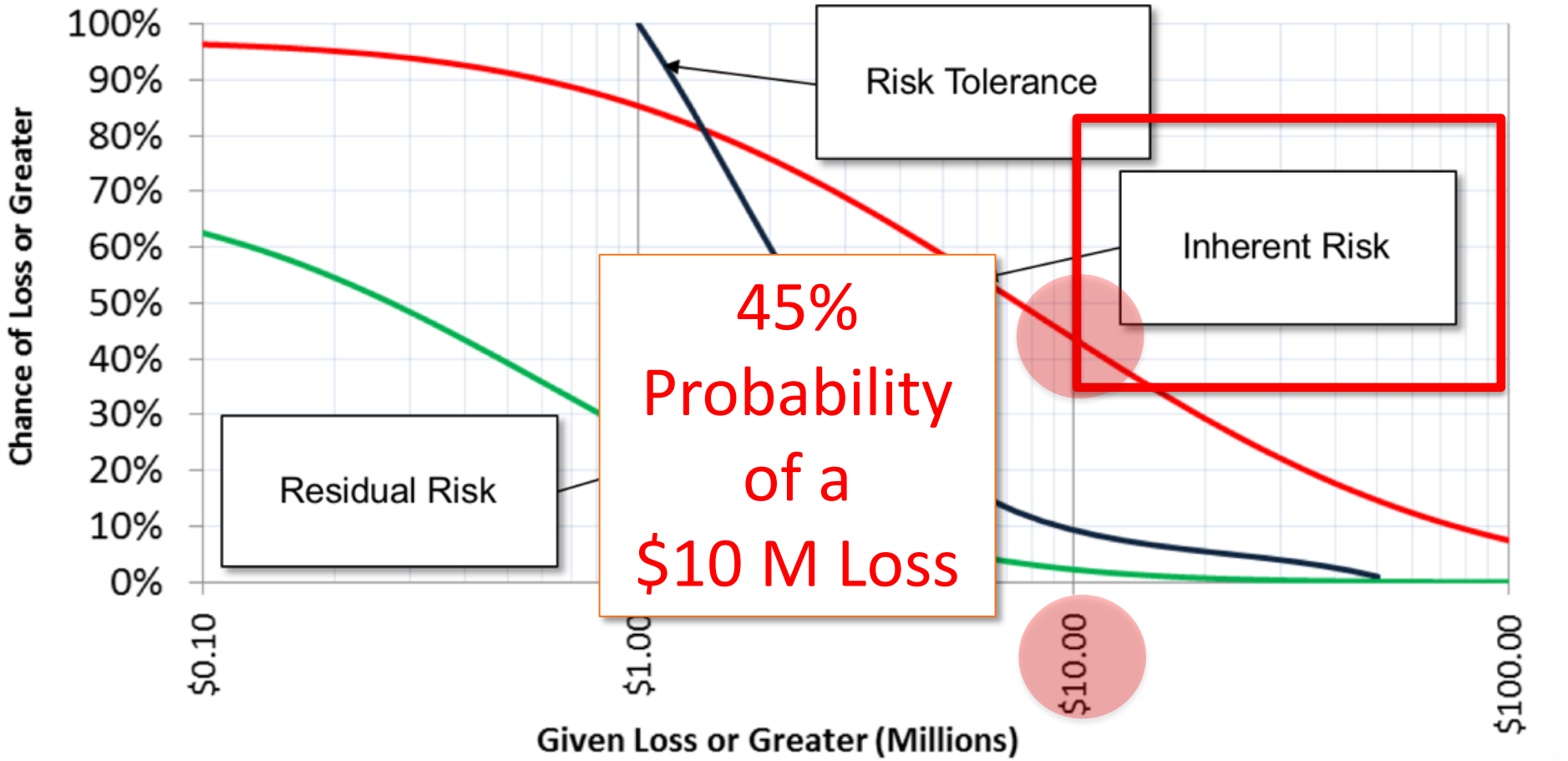
97% Probability of a $10K Loss



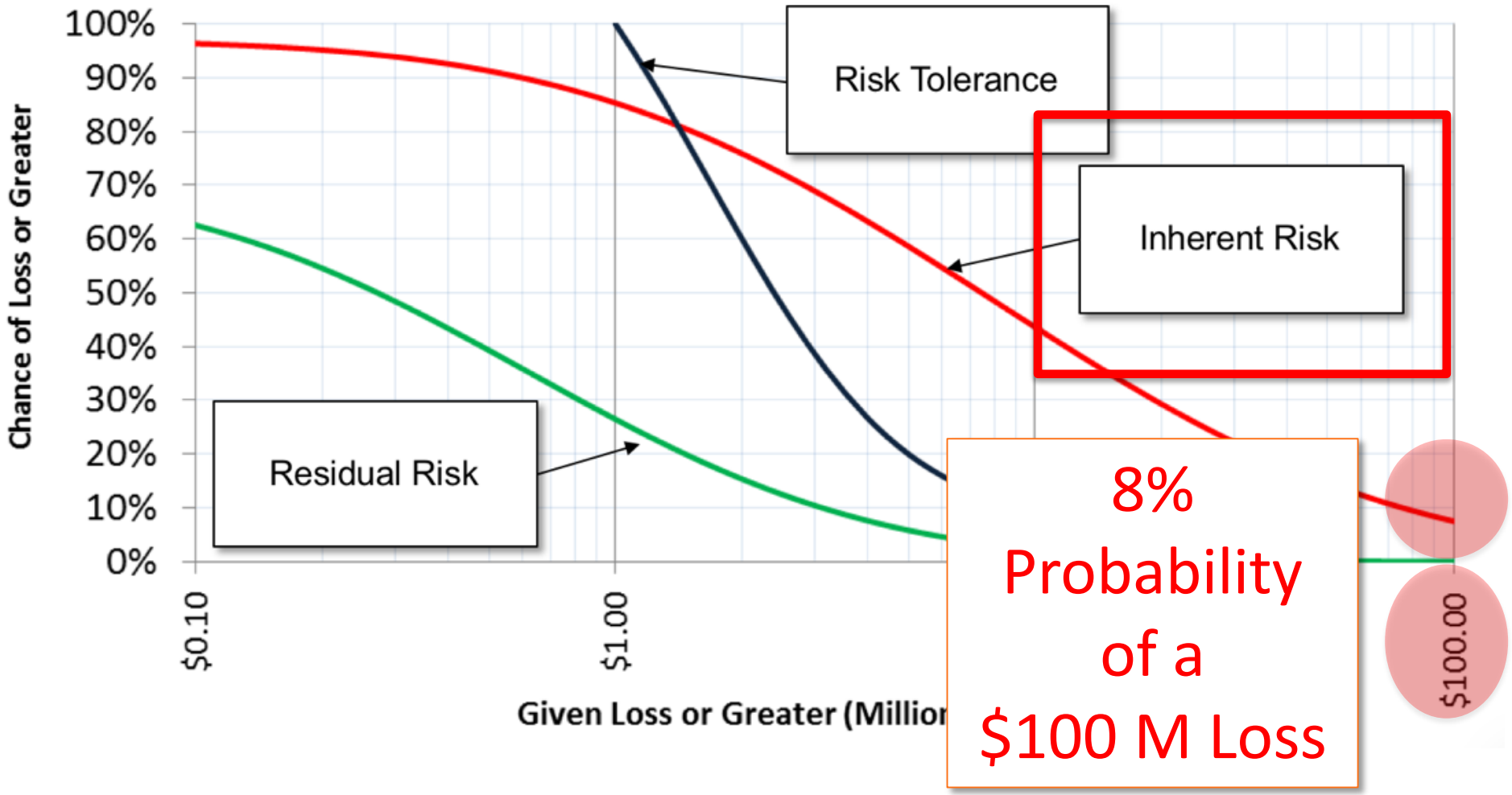
Loss Exceedance Curves



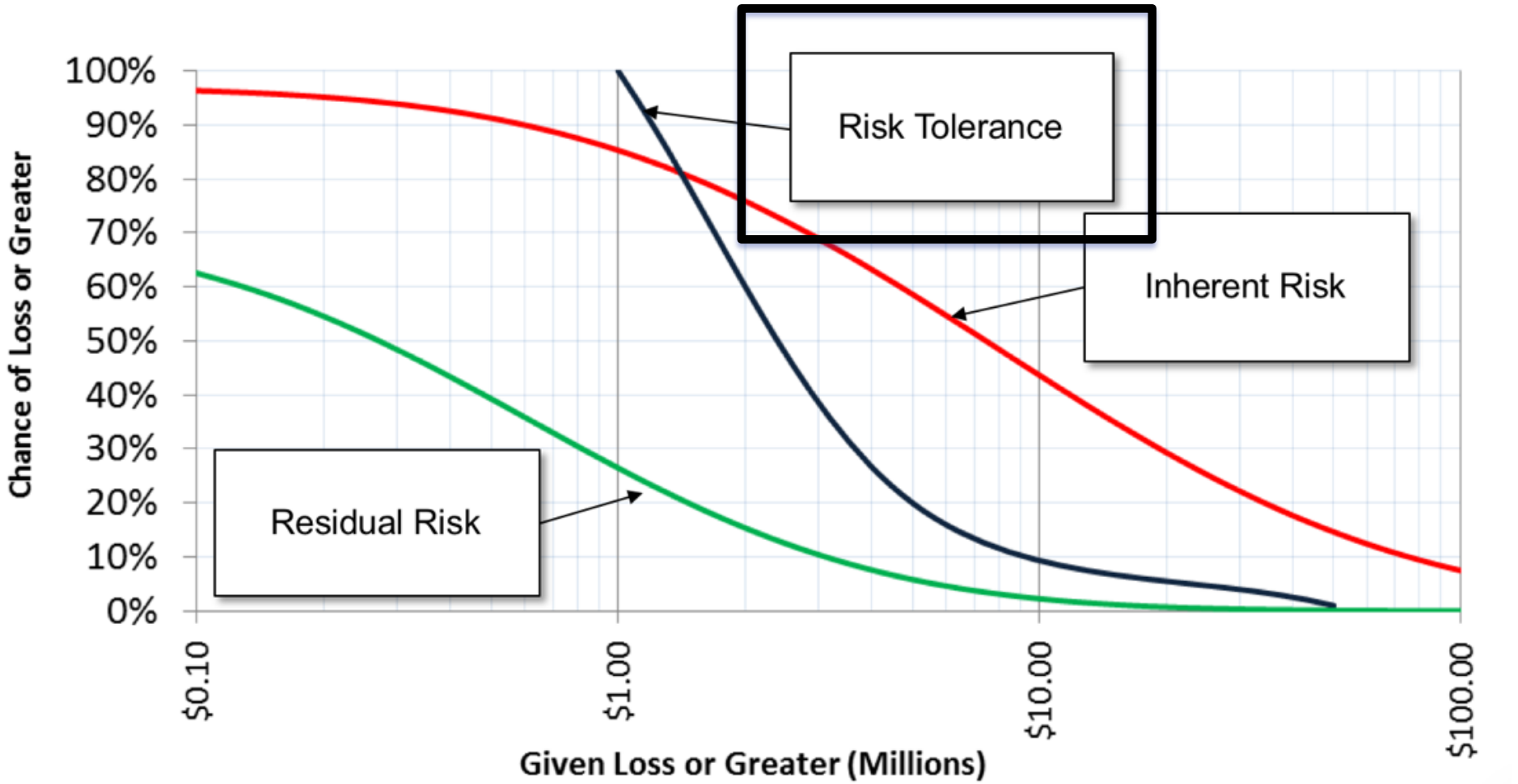
Loss Exceedance Curves



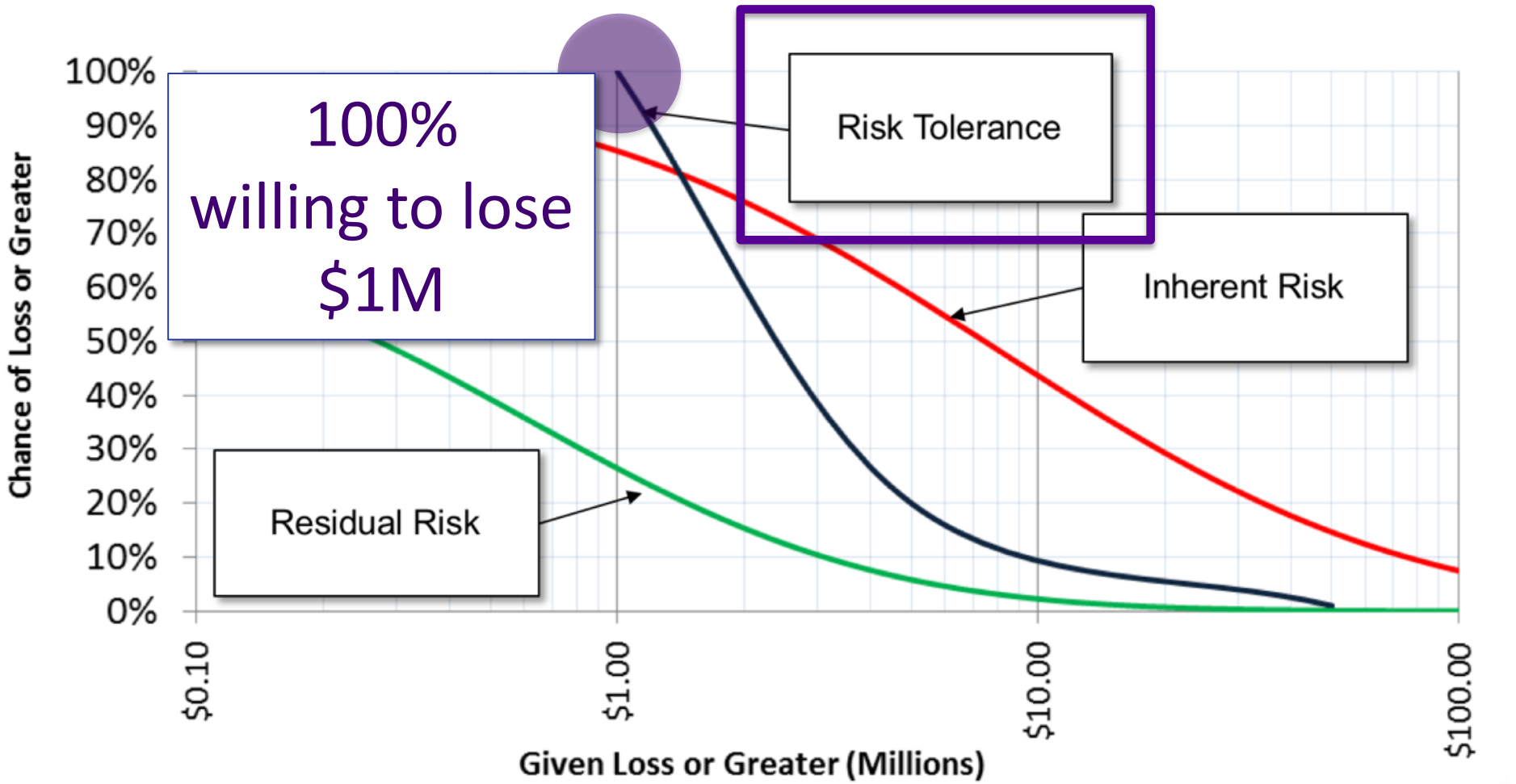
Loss Exceedance Curves



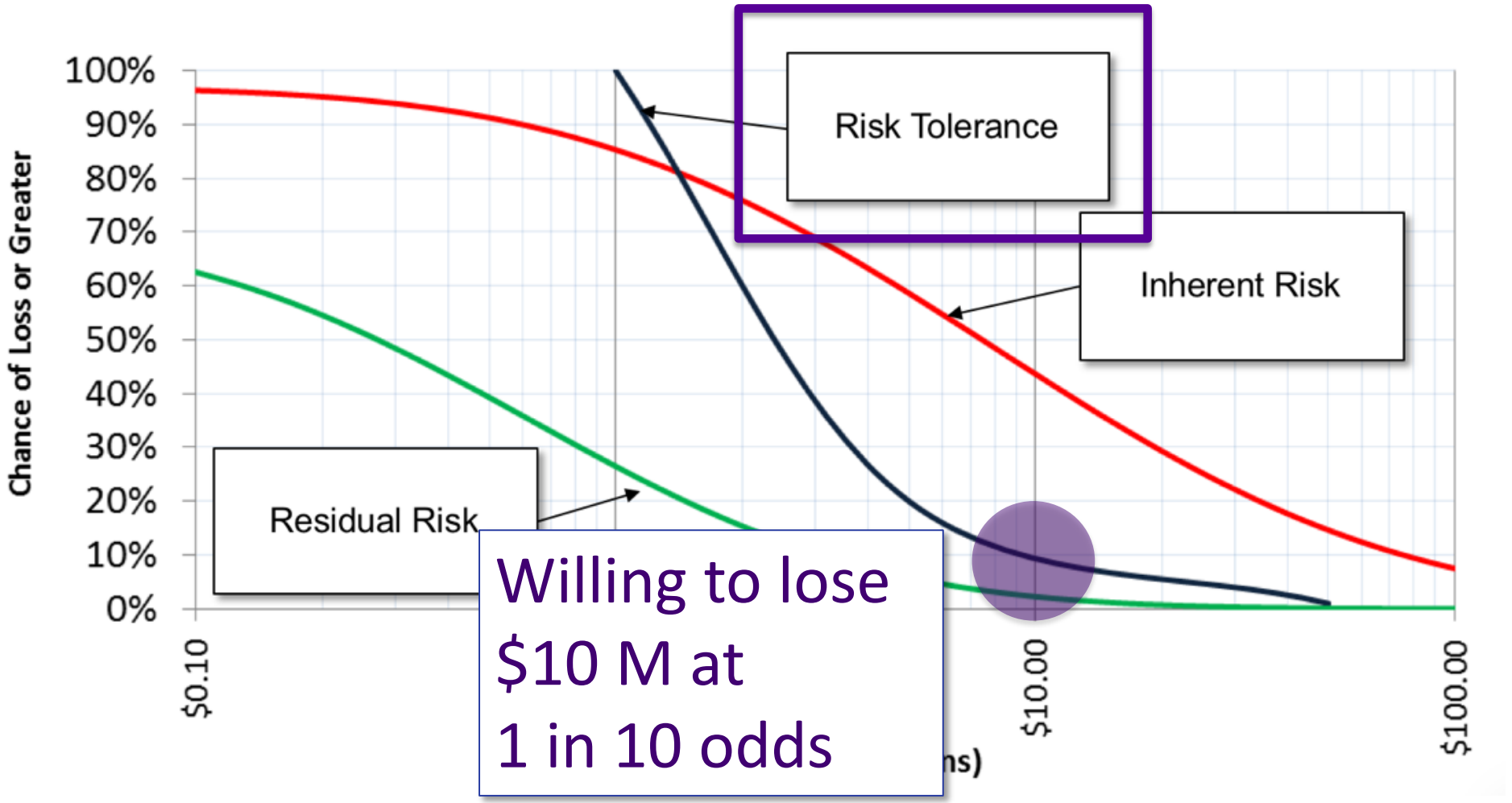
Loss Exceedance Curves



Loss Exceedance Curves

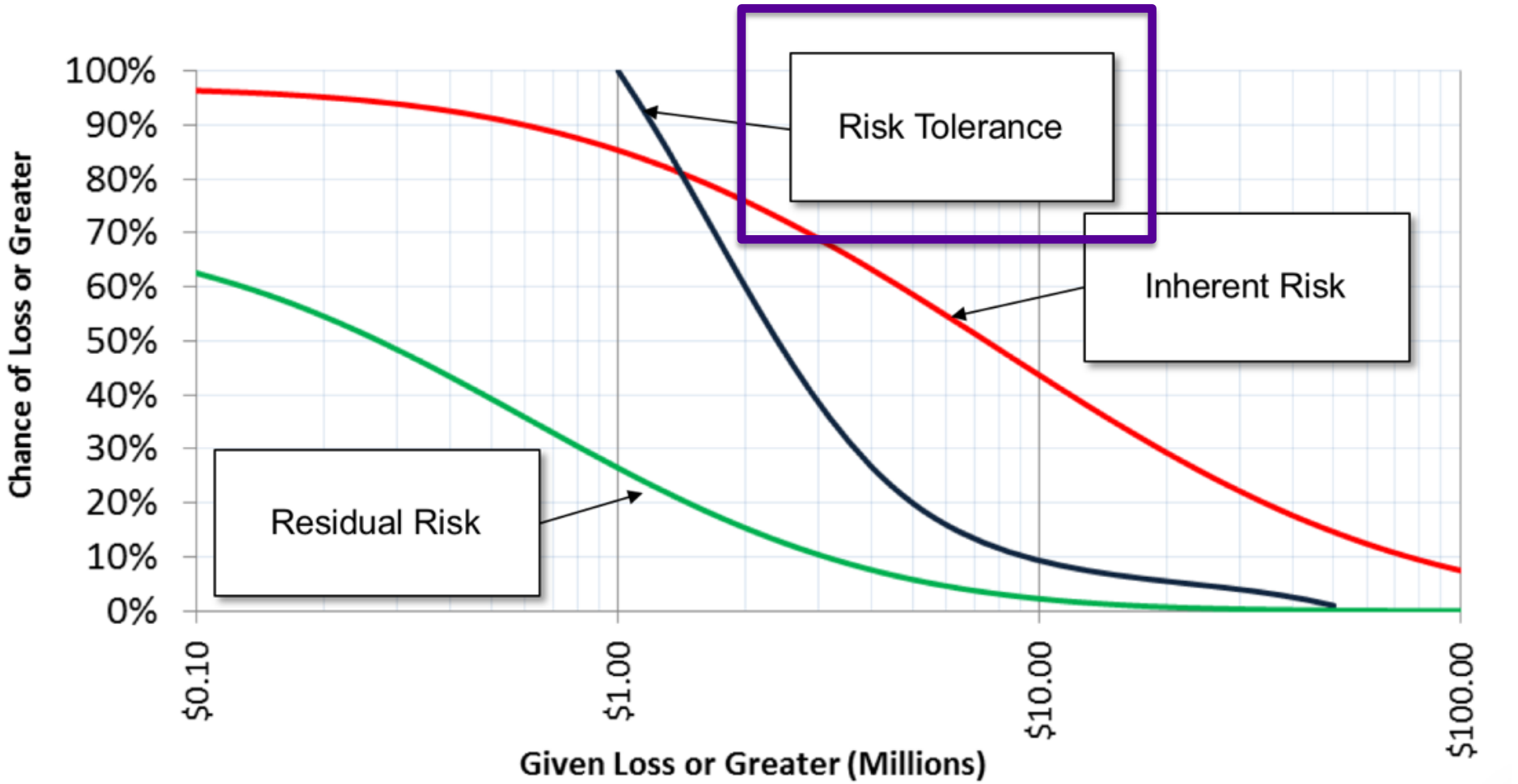


Loss Exceedance Curves

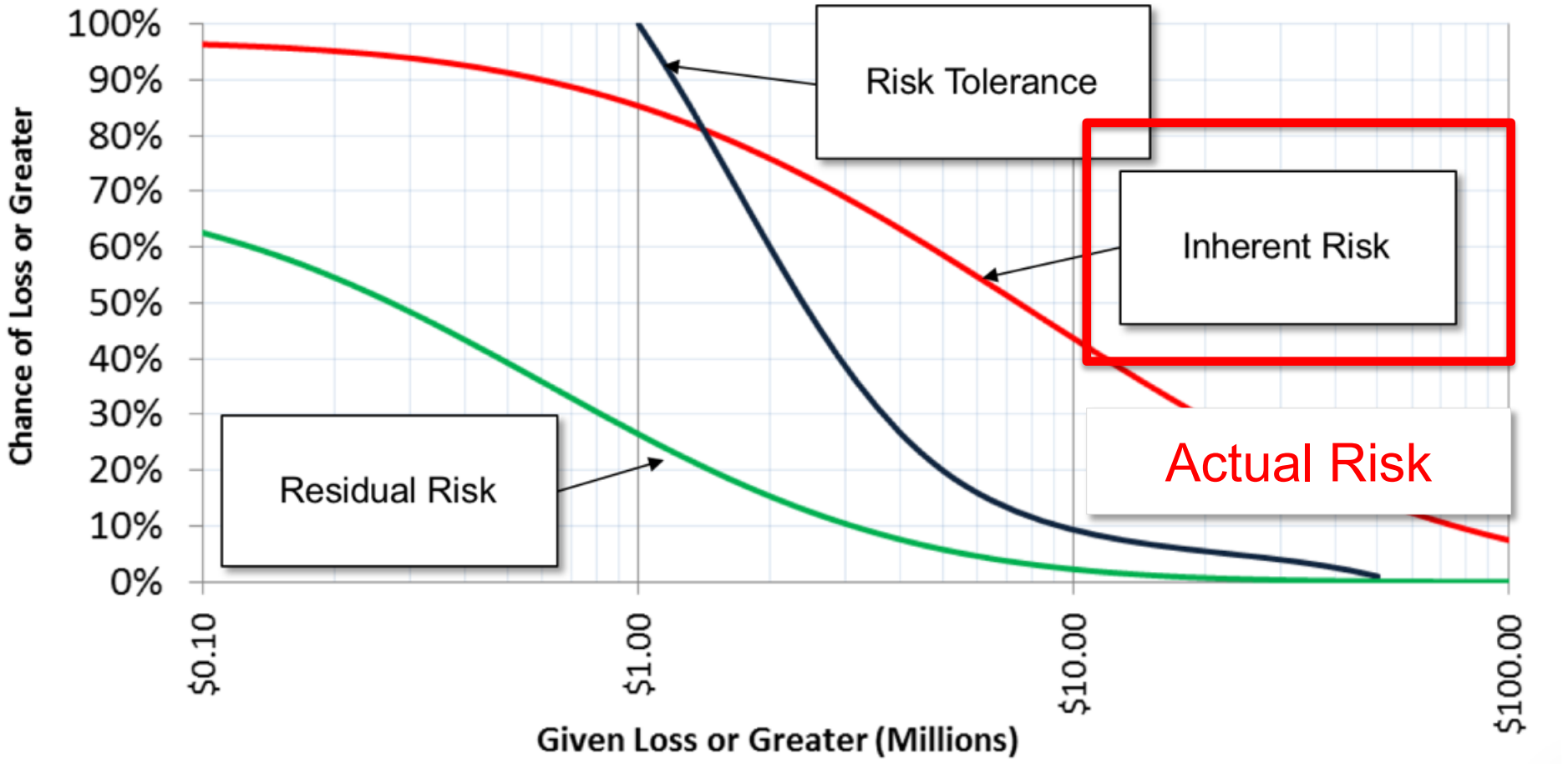


Loss Exceedance Curves

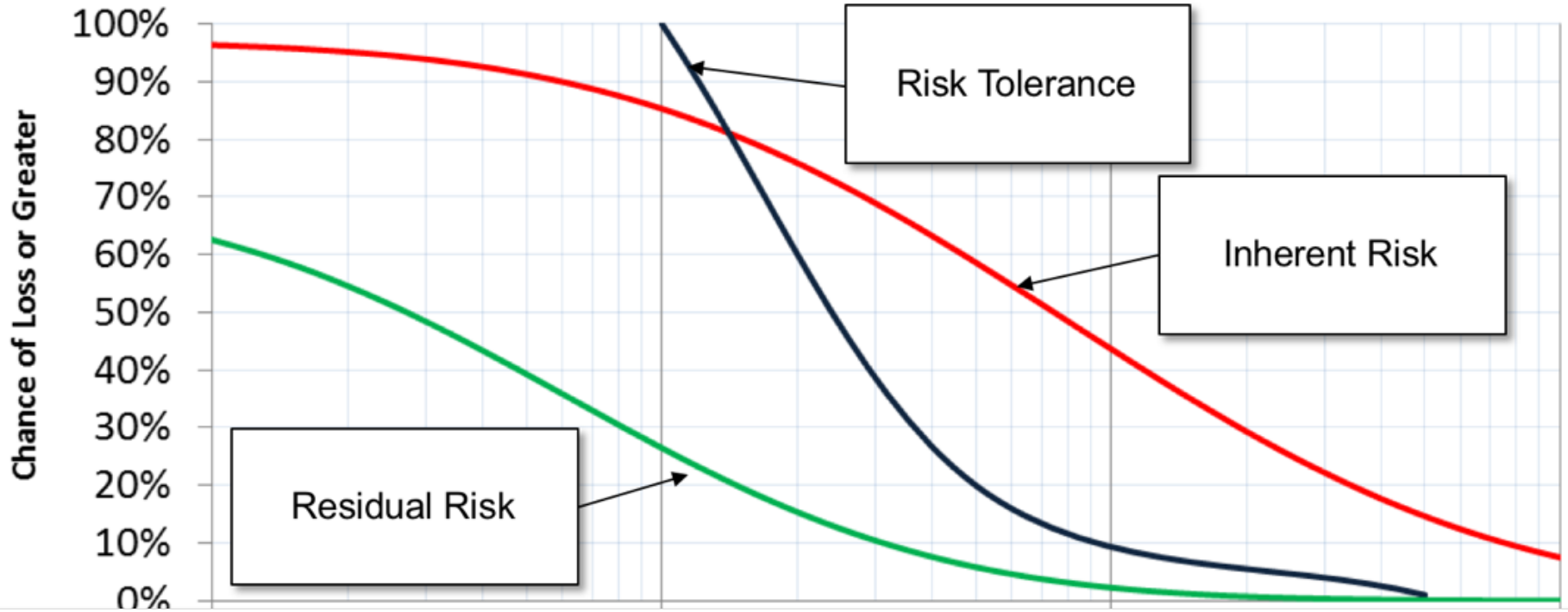
Accepted Risk



Loss Exceedance Curves

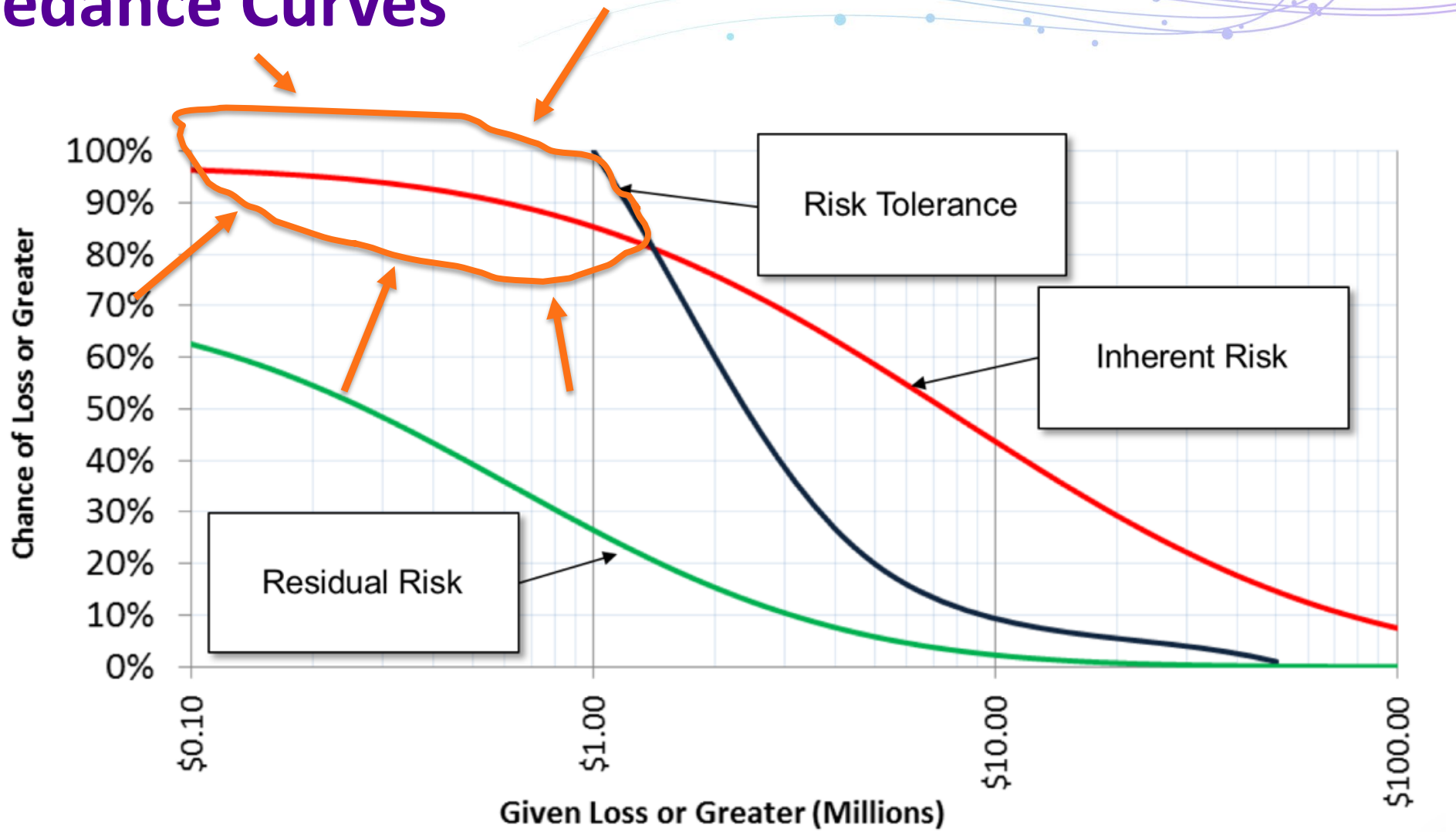


Loss Exceedance Curves

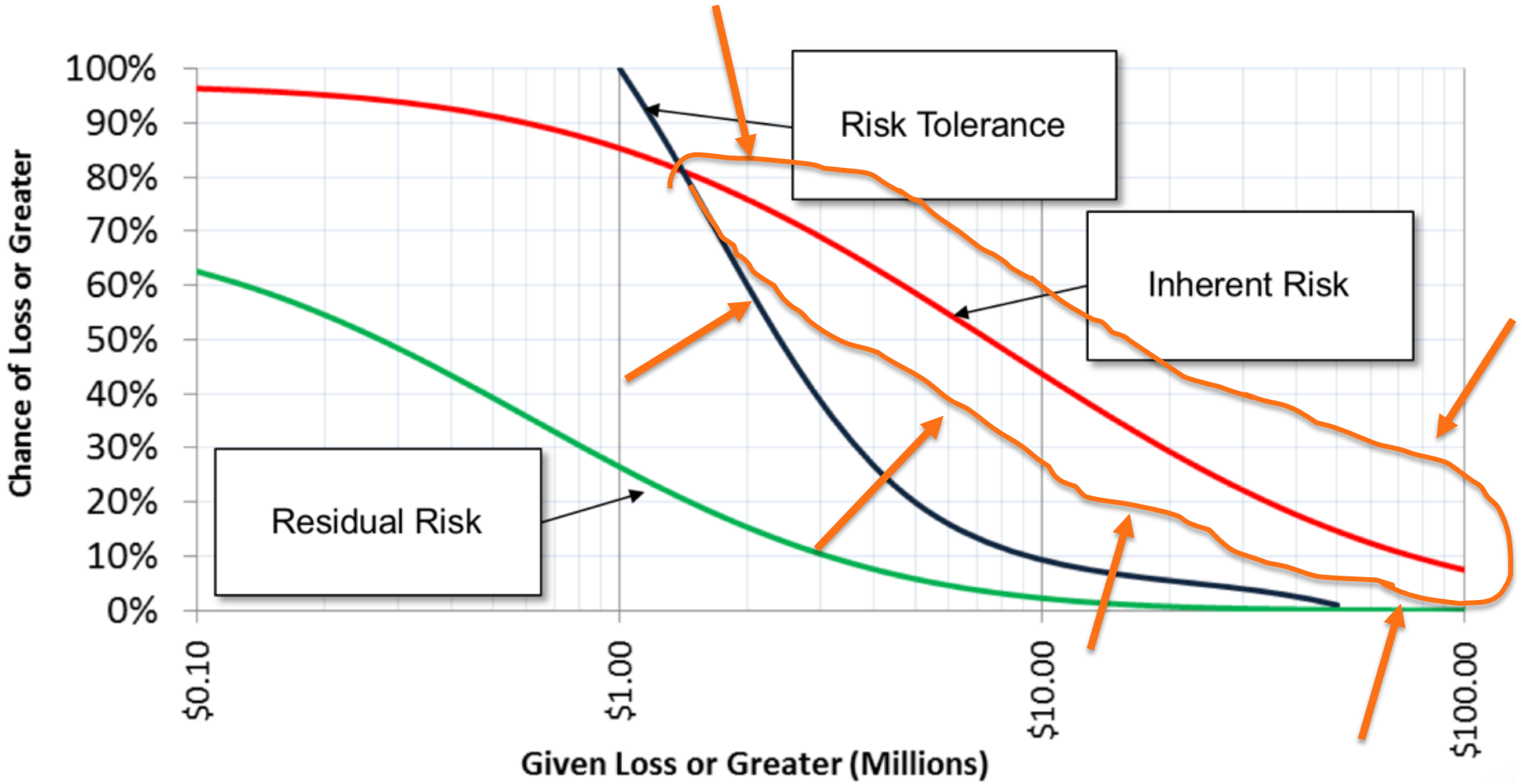


Accepted Risk ≠ Actual Risk

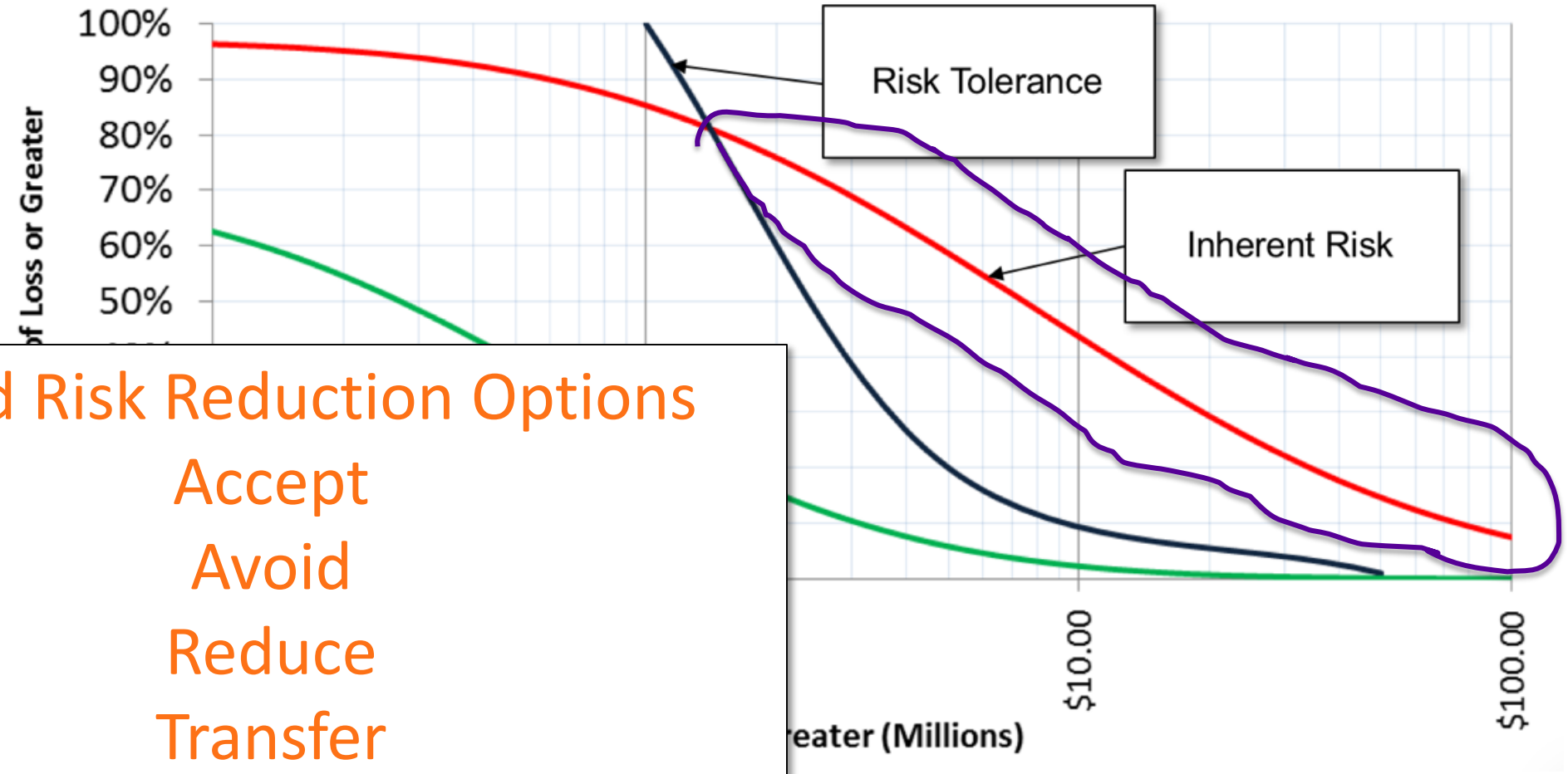
Loss Exceedance Curves



Loss Exceedance Curves



Loss Exceedance Curves



Board Risk Reduction Options

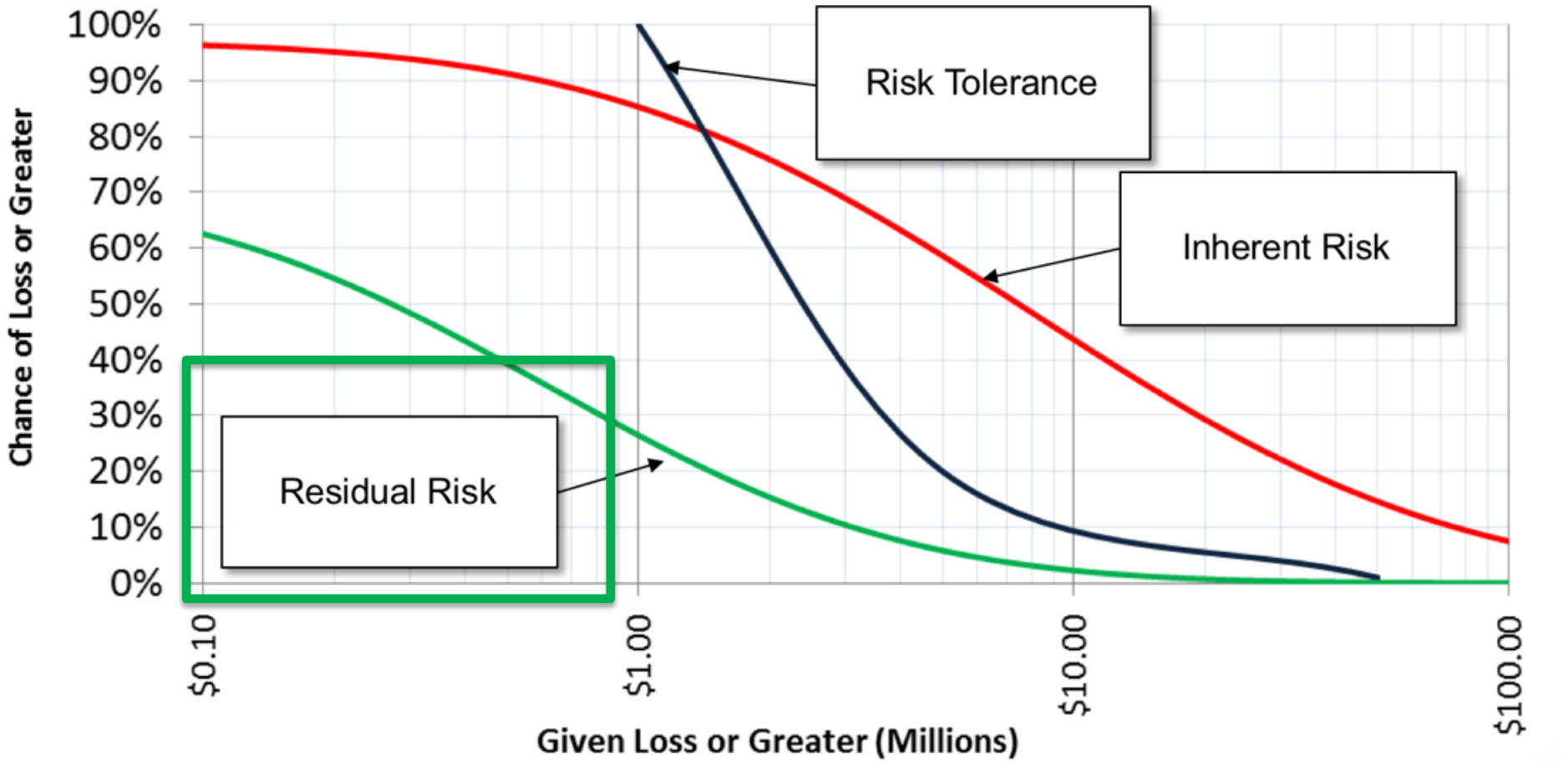
Accept

Avoid

Reduce

Transfer

Loss Exceedance Curves



Transition

RSAConference2019

Getting Ready for the Board

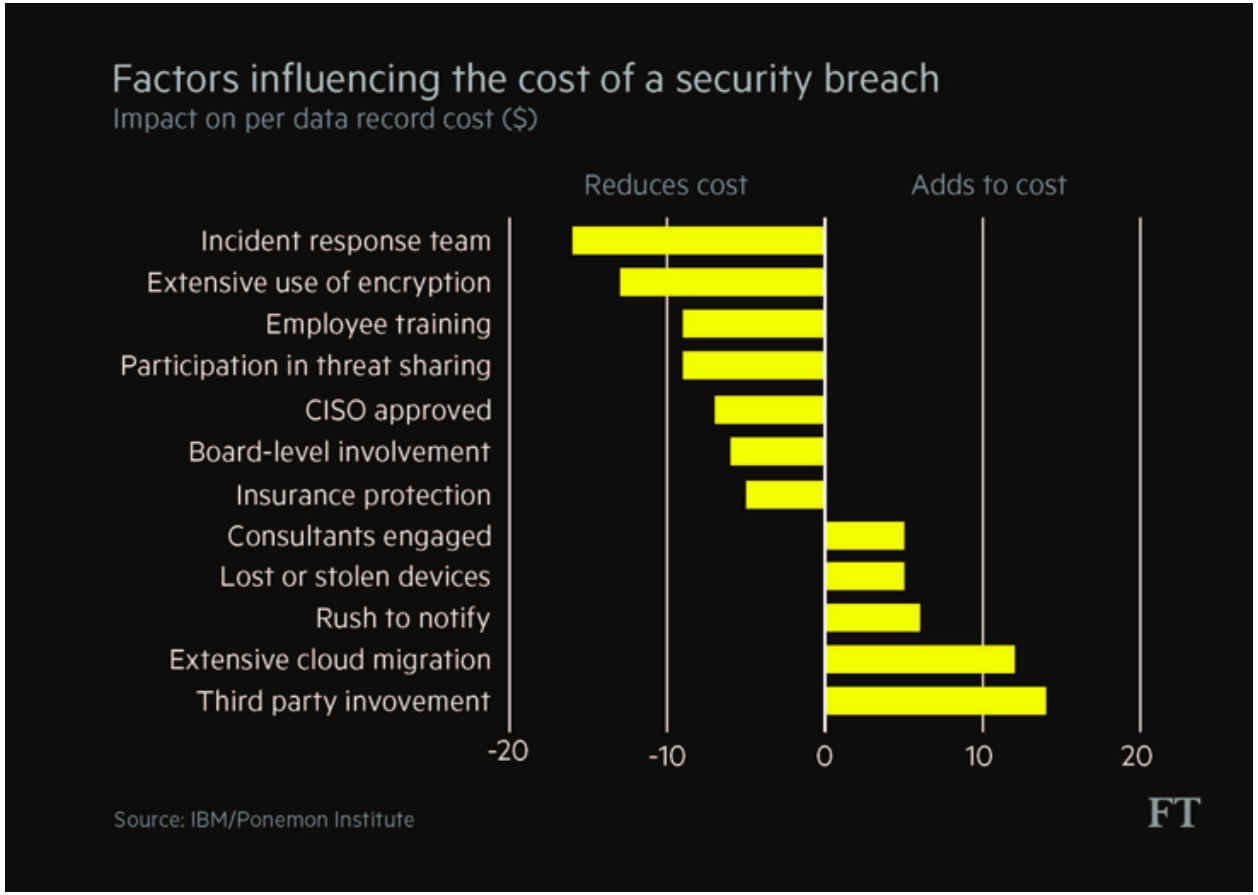
Preparing for the Board Step by Step

Preparing for the Board Step by Step

1: Determine the current cost of the existing security program.

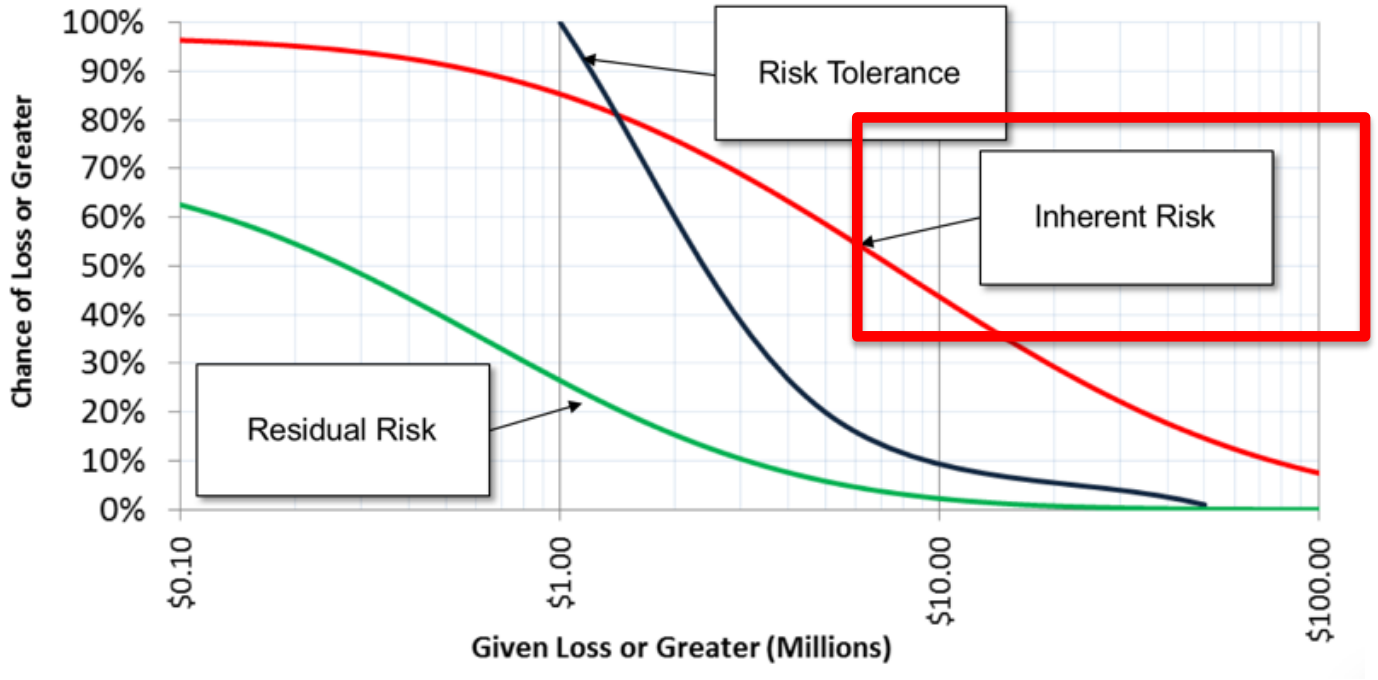
Preparing for the Board Step by Step

2: Estimated the cost after the boom.



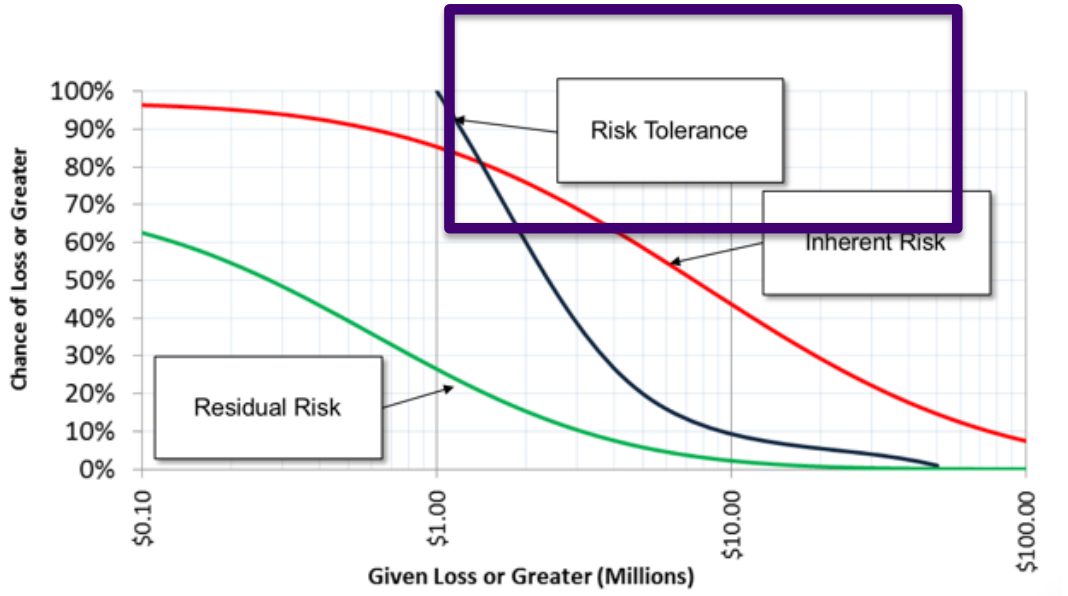
Preparing for the Board Step by Step

3: Build the Inherent Risk Curve.



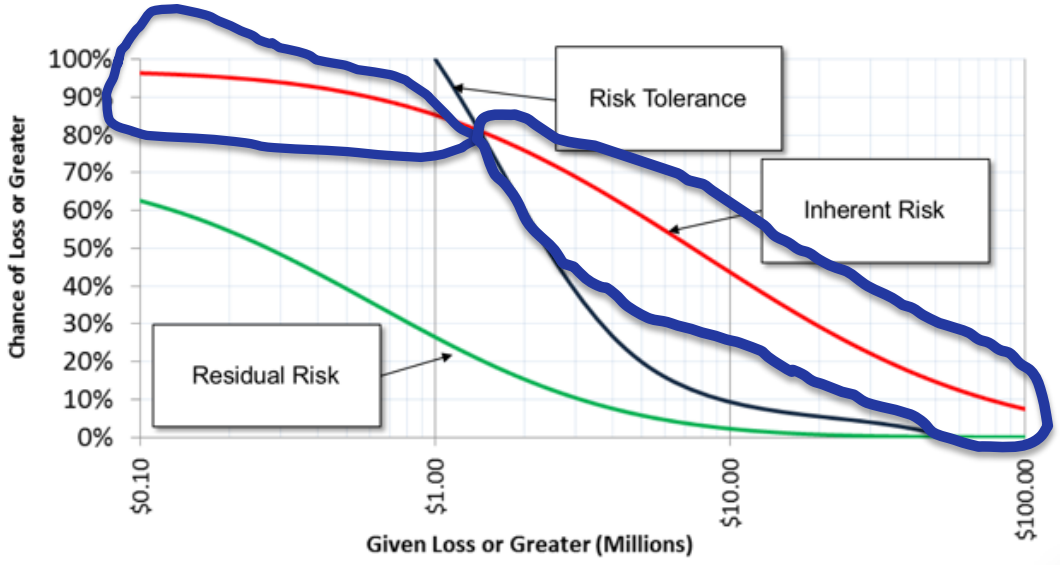
Preparing for the Board Step by Step

4: Build the Risk Tolerance Curve.



Preparing for the Board Step by Step

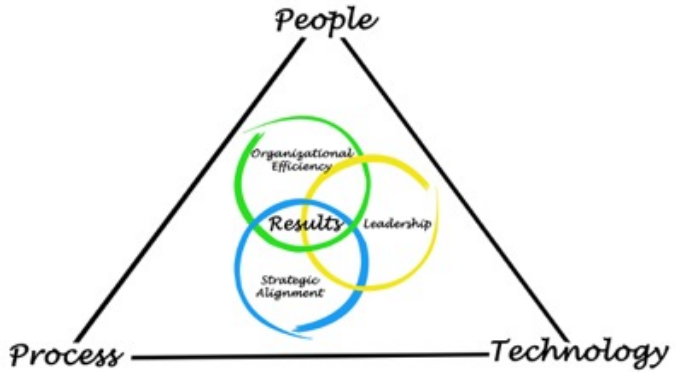
5: Overlay the Two Curves: Inherent Risk and Risk Tolerance.



Preparing for the Board Step by Step

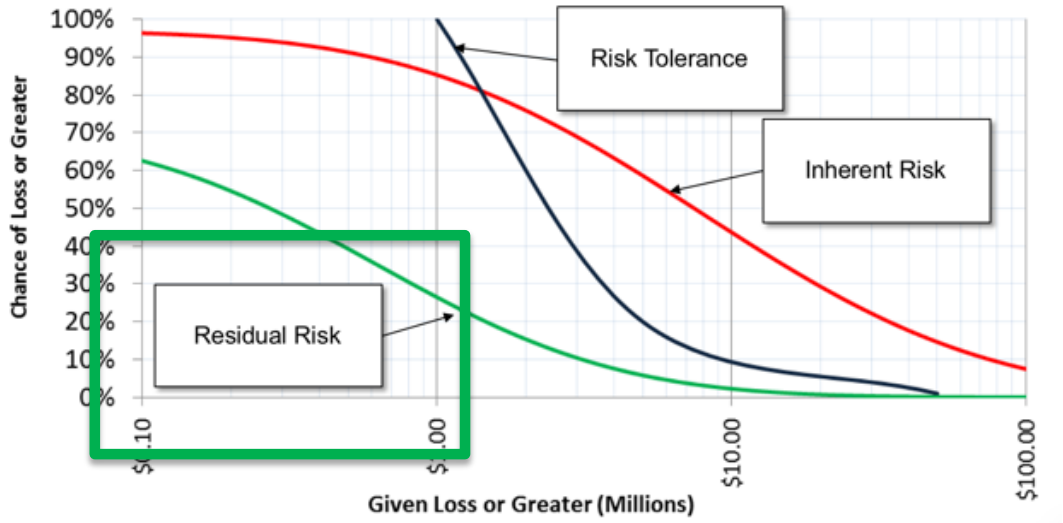
6: If the Inherent Risk < Risk Tolerance, do nothing.

Preparing for the Board Step by Step



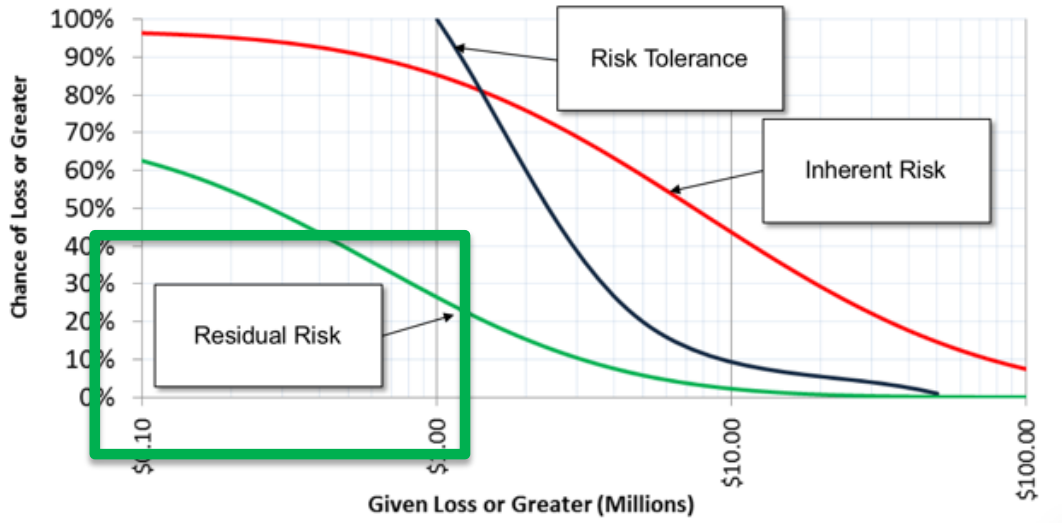
7: If the Inherent Risk > Risk Tolerance, Develop Strategy to Reduce Risk.

Preparing for the Board Step by Step



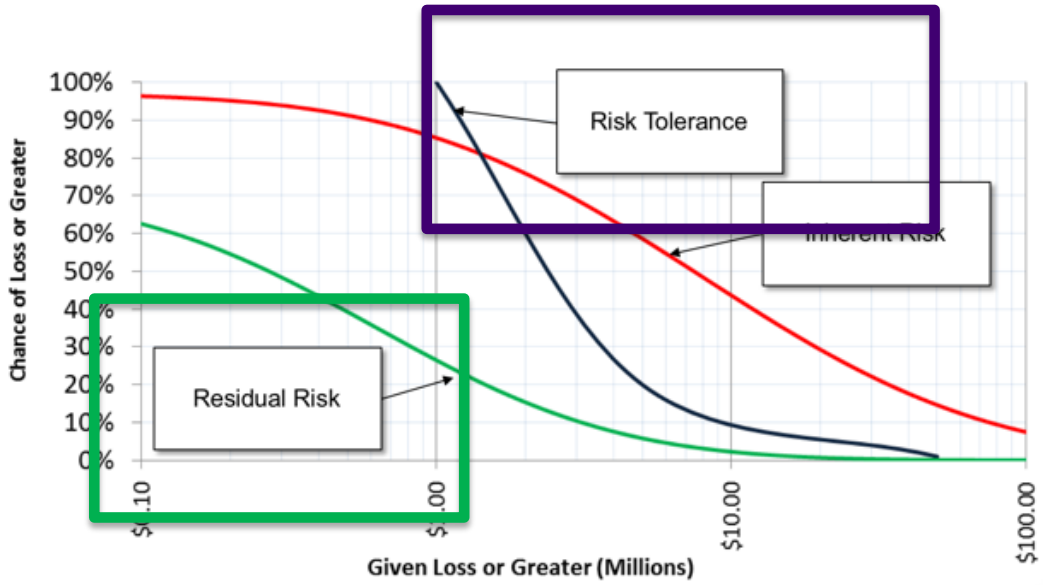
8: Build the Residual Risk Curve.

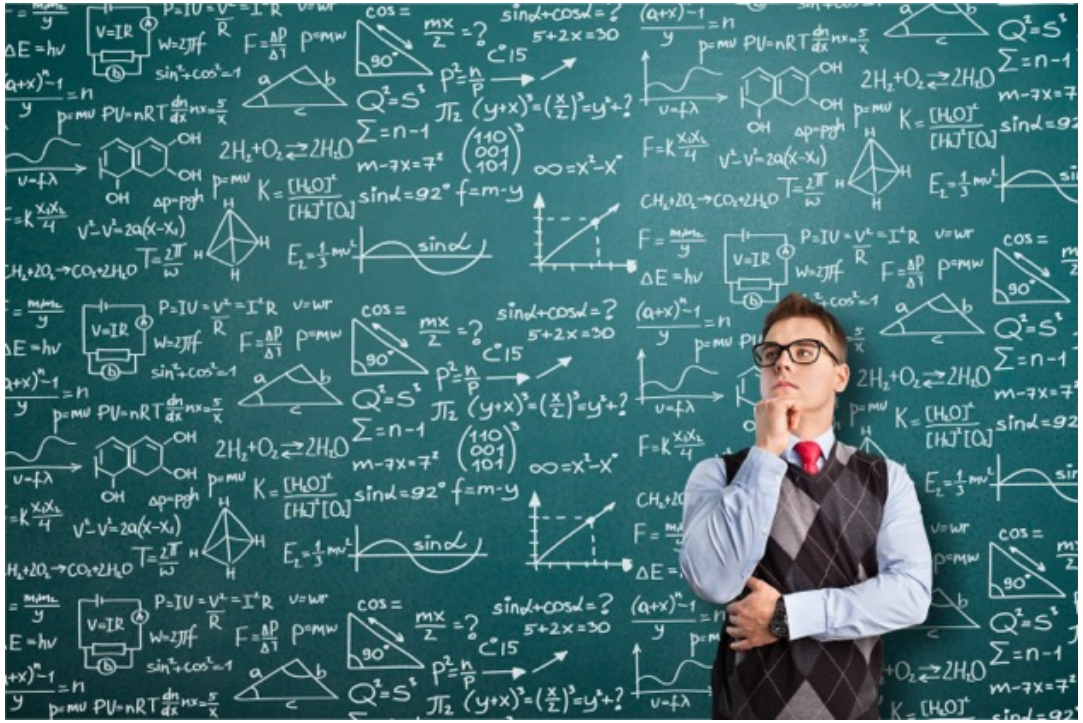
Preparing for the Board Step by Step



9: Calculate the cost of the new strategy.

Preparing for the Board Step by Step





10: If the Cost of the Residual Risk Plan > the Risk Tolerance Curve, Start Over.

Preparing for the Board Step by Step

11: For each Board Meeting, Rinse and Repeat.

Preparing for the Board Step by Step

1: Determine the current cost of the existing security program.

2: Estimated the cost after the boom.

3: Build the Inherent Risk Curve.

4: Build the Risk Tolerance Curve.

5: Overlay the Two Curves: Inherent Risk and Risk Tolerance.

6: If the Inherent Risk < Risk Tolerance, do nothing.

7: If the Inherent Risk > Risk Tolerance, Develop Strategy to Reduce Risk.

8: Build the Residual Risk Curve.

9: Calculate the cost of the new strategy.

10: If the Cost of the Residual Risk Plan > the Risk Tolerance Curve, Start Over.

11: For each Board Meeting, Rinse and Repeat.

Transition

RSAConference2019

How to Build Latency Curves

Warning: The following will contain some math.

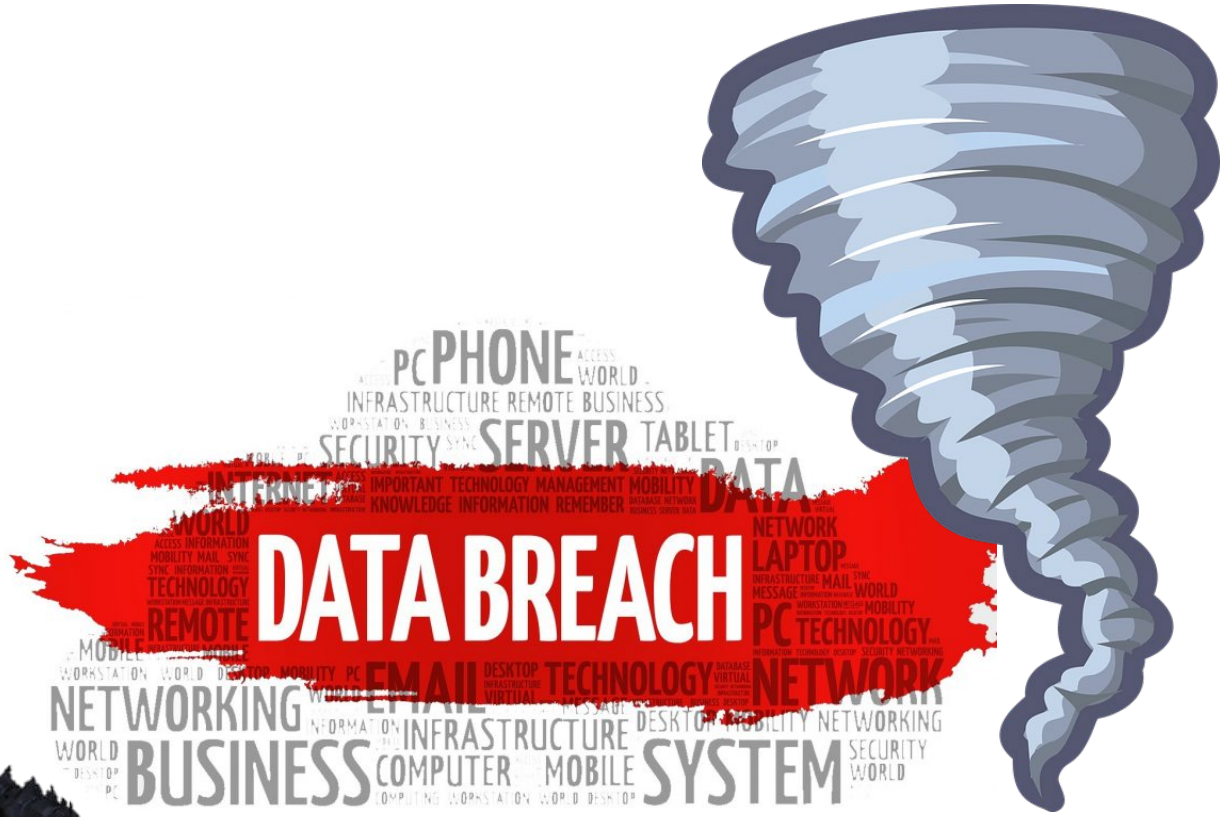
Not a lot though, and it’s very doable.

We’ve even given you a spreadsheet to help!

Building a curve for Loss Exceedance

1: Identify your organization's Risk Register Items.

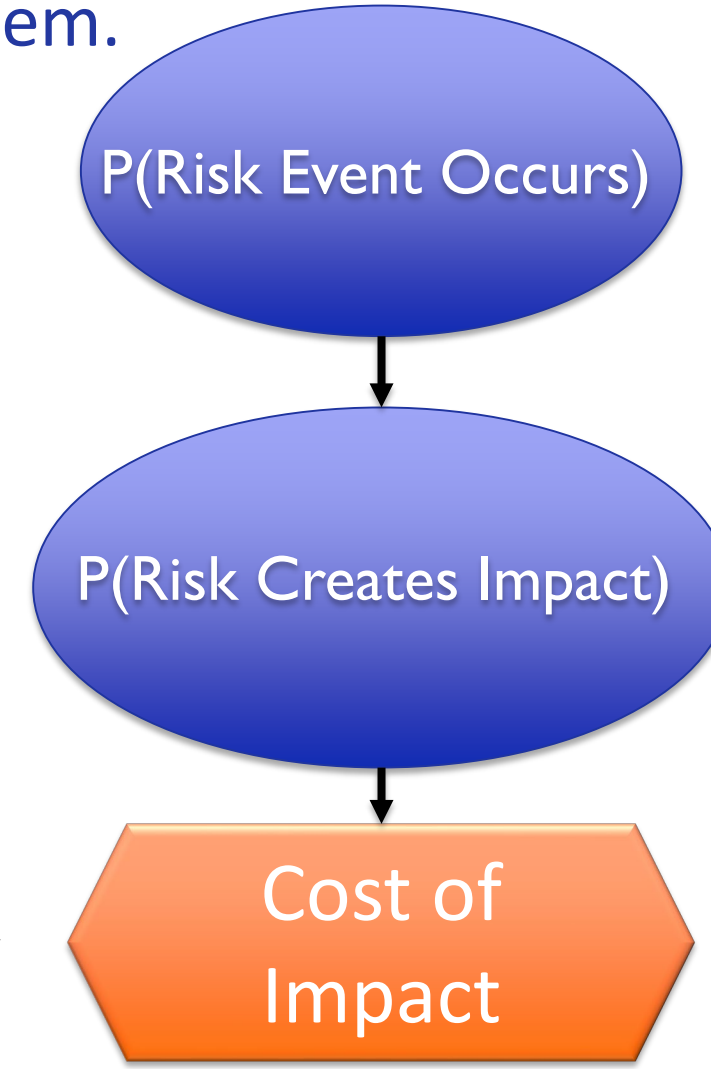
- What are the key Events of concern?
- What is your timeframe?



Building a curve for Loss Exceedance

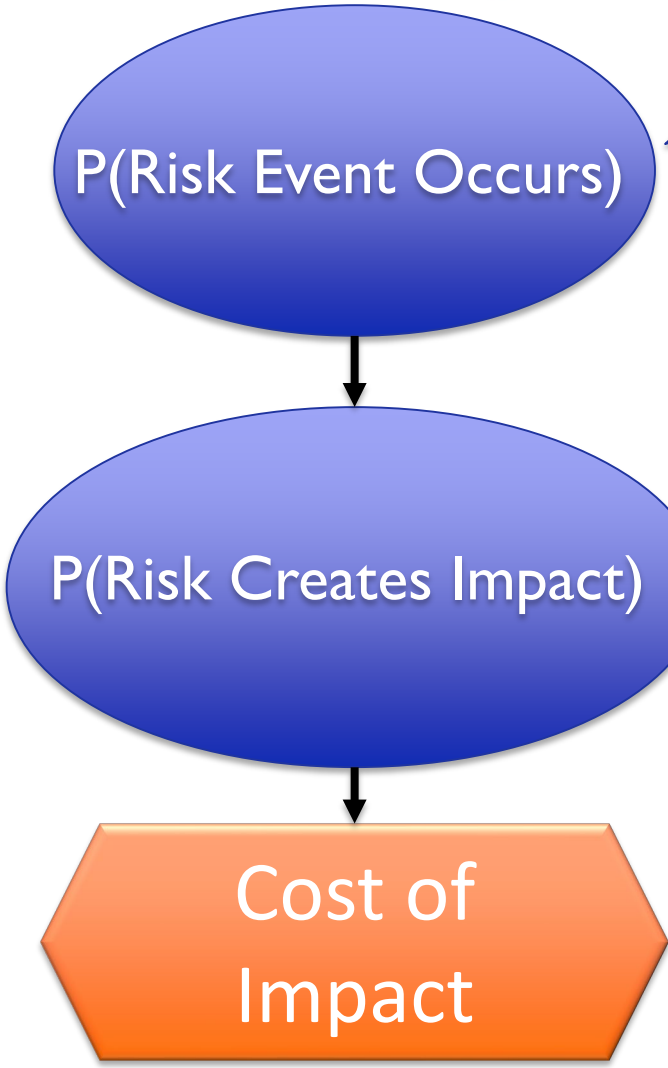
2: Assess the probability of occurrence/impact for each Item.

Risk	Description
1	Loss of customer records due to a cyber event in the next three years?
2	A large scale power outage (>72 hours) with our data center within the next 3 years?
…	
N	Godzilla crushes the company data center in the next three years?



Circles: Information Uncertainty

Hexes: Values



What is the probability that there will be a large scale power outage (>72 hours) with our data center within the next 3 years?

P(Power Outage >72 hours in next 3 years)

What is the probability that the large scale power outage within the next 3 years will create a material loss?

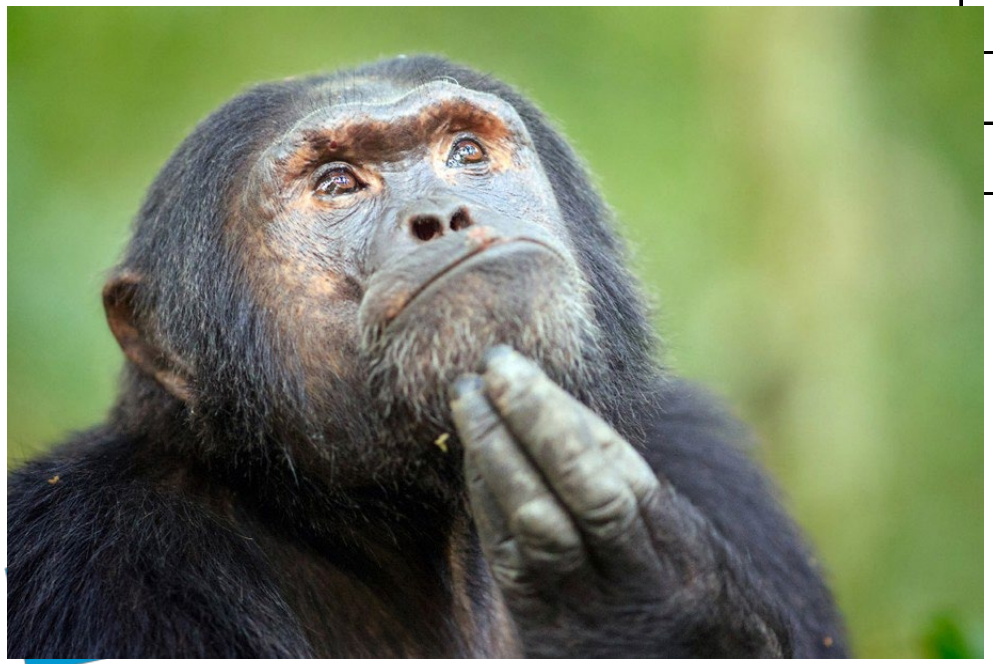
P(Material Loss ($M) |
Large Power Outage >72 hours in next 3 years)

Building a curve for Loss Exceedance

3: Assess the probability of various loss levels given the Item occurs.

Loss Amount ($M)	Probability of Loss Given Event Occurs and Material Impact
$0	--
>0 and <=1	0.6
>1 and <=2	0.3
>2 and <=5	0.1

=1



Building a curve for Loss Exceedance

4: Calculate the posterior probability loss distribution for each item.

P(Event Occurs) = 0.05

P(Material Impact | Event Occurs) = 0.9

P(Material Impact and Event Occurs) = 0.05 * 0.9 = 0.045

Loss Amount ($M)	Probability of Loss Given Event Occurs and Material Impact	Posterior Probability of Loss
$0		0.955
>0 and <=1	0.6	0.027
>1 and <=2	0.3	0.014
>2 and <=5	0.1	0.005

0.045 * 0.6

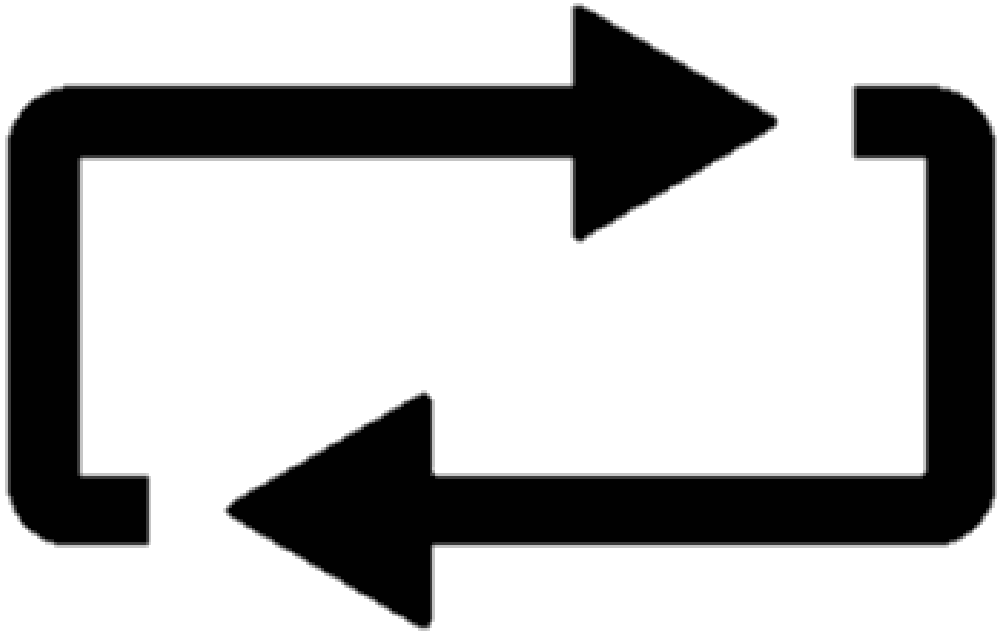
Building a curve for Loss Exceedance

5: Convert the previous to a cumulative distribution function (CDF) of loss.

Loss Amount ($M)	Probability of Loss Given Event Occurs and Material Impact	Posterior Probability of Loss	Cumulative Probability of Loss
$0	--	0.955	0.955
>0 and <=1	0.6	0.027	0.982
>1 and <=2	0.3	0.014	0.995
>2 and <=5	0.1	0.005	1

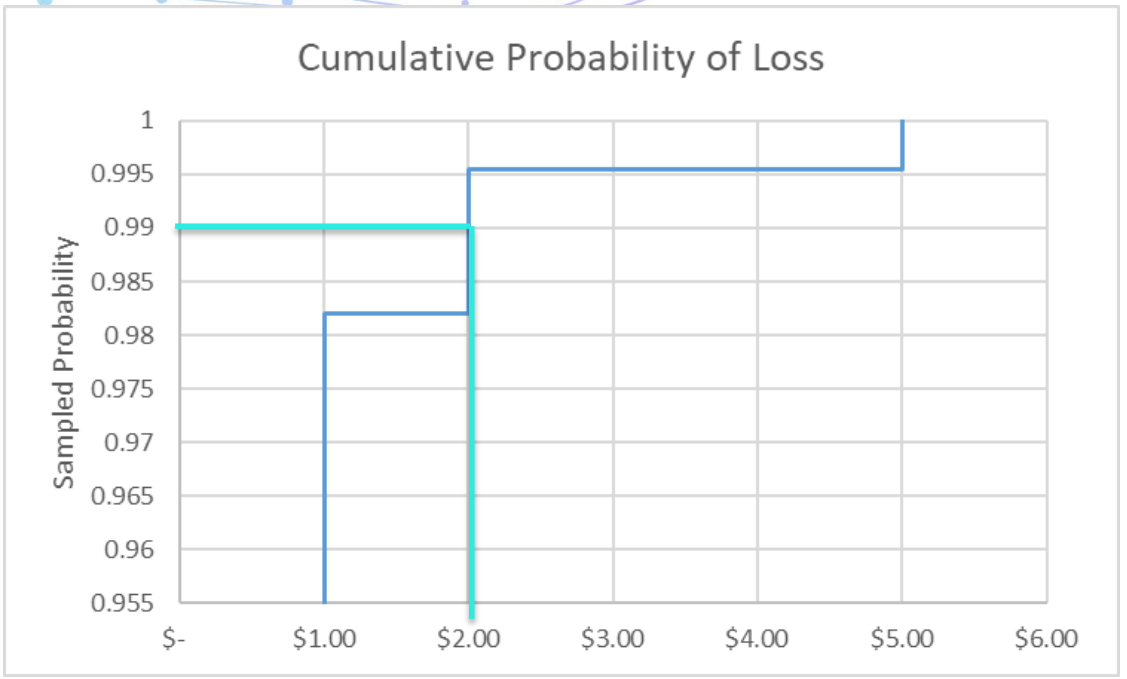
Building a curve for Loss Exceedance

6: Repeat 2-5 for every Risk Register Item.



Building a curve for Loss Exceedance

0.99



7: Sample the CDFs to generate sample losses.

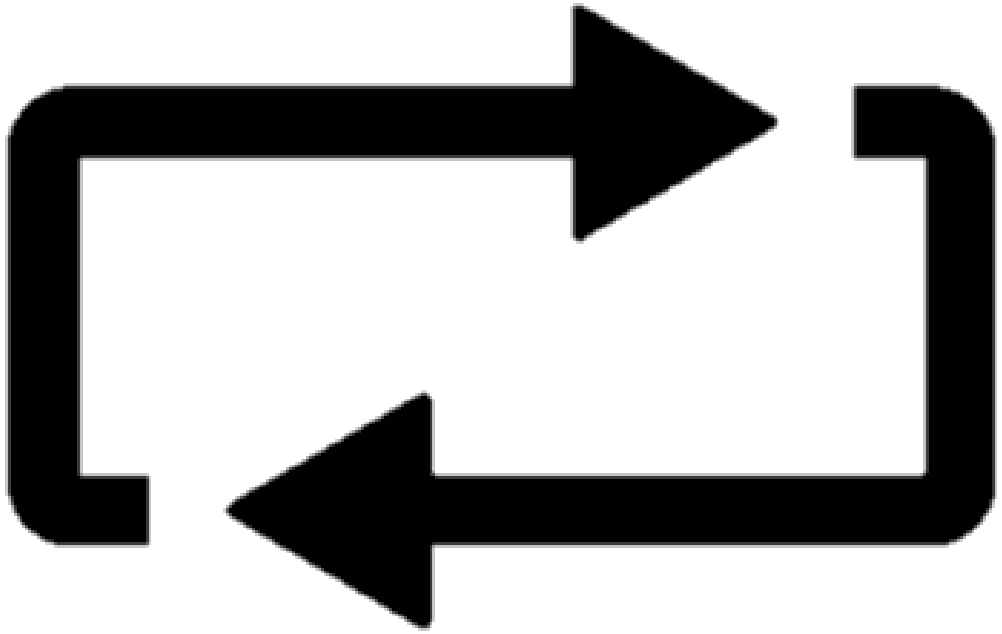
$2M Loss

Building a curve for Loss Exceedance

$2M + $0M + $0M + $0M + $5M = $6M

8: Add each of the Item's sampled losses => total loss for the sample.

Building a curve for Loss Exceedance

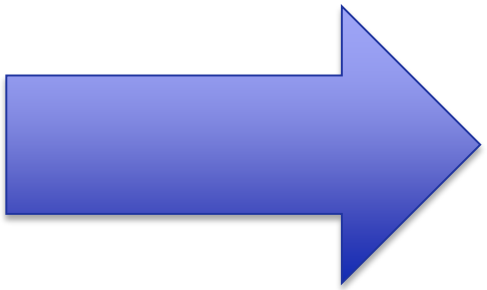


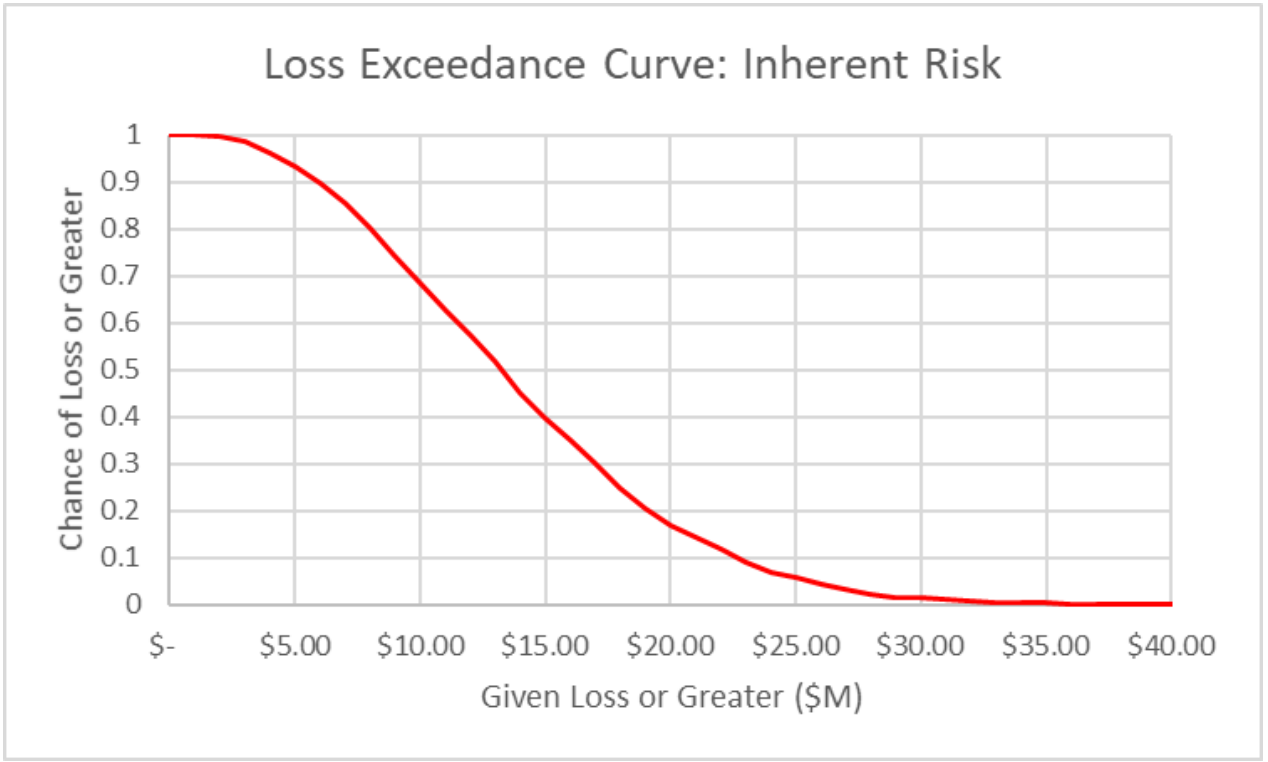
9: Repeat 7-8 a couple 100,000's of times (this is Monte Carlo sampling!)

Building a curve for Loss Exceedance

Total Loss Amount ($M)	Count of Samples	% of Samples
$ -	11	0.000711
$ 1	75	0.00485
$ 2	181	0.011704
$ 3	342	0.022114
$ 4	489	0.03162
$ 5	546	0.035306
$ 6	630	0.040737
$ 7	749	0.048432

…





10: Convert the count of each sample value into probability and plot.

Building a curve for Loss Exceedance

1: Identify your organization's Risk Register Items.

2: Assess the probability of occurrence/impact for each Item.

3: Assess the probability of various loss levels given the Item occurs.

4: Calculate the posterior probability loss distribution for each item.

5: Convert the previous to a cumulative distribution function (CDF) of loss.

6: Repeat 2-5 for every Risk Register Item.

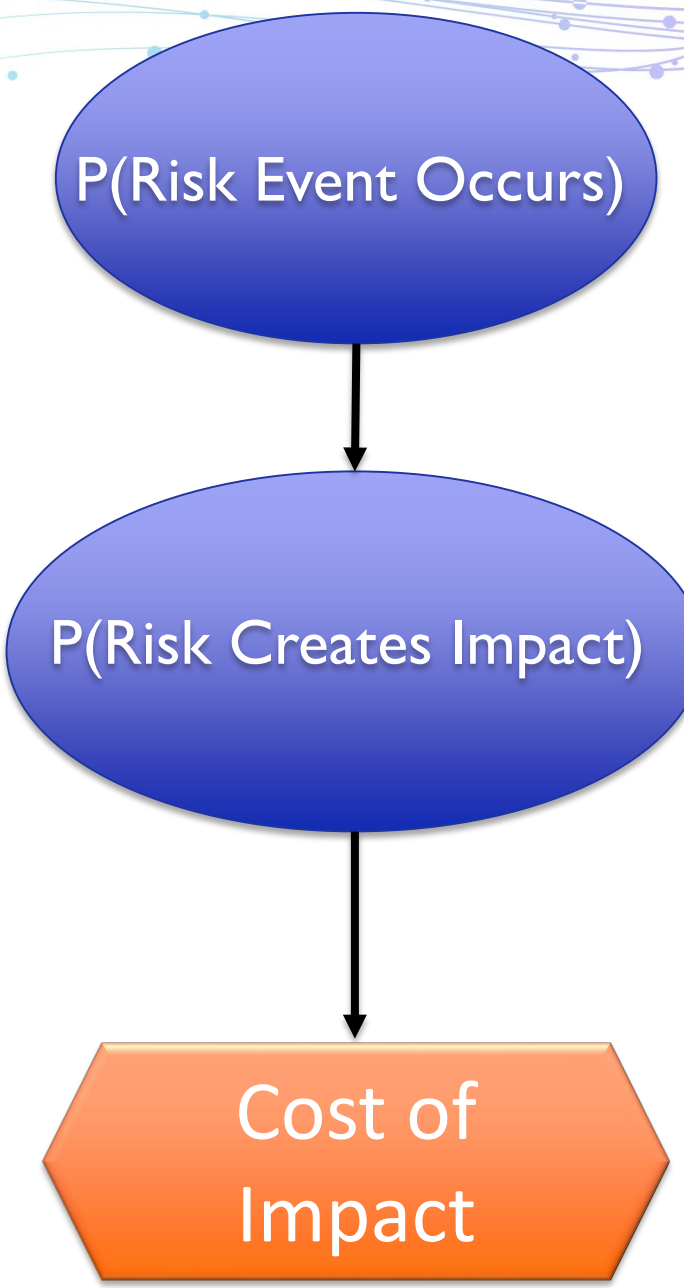
7: Sample the CDFs to generate sample losses.

8: Add each of the Item's sampled losses => total loss for the sample.

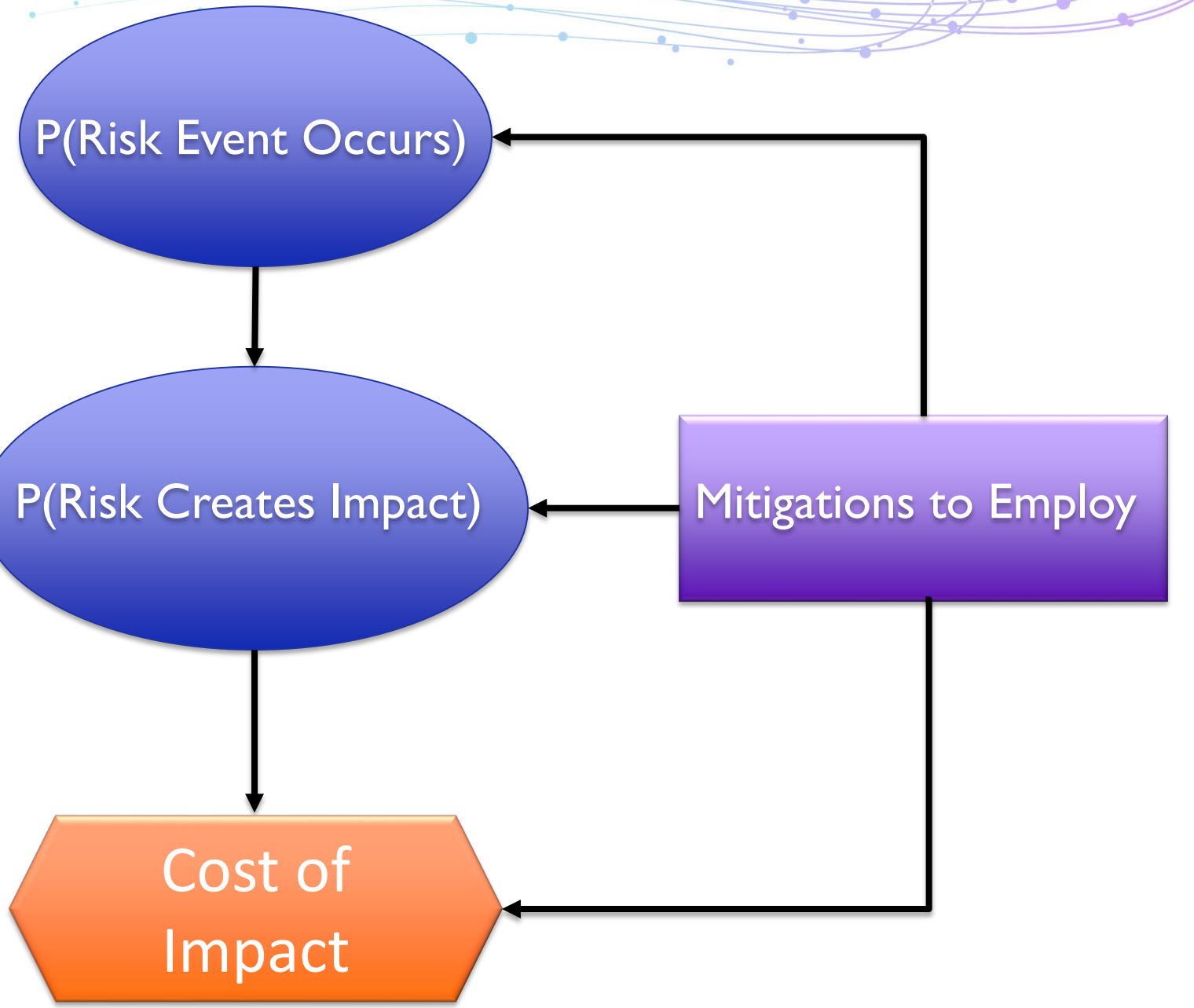
9: Repeat 7-8 a couple 100,000's times (this is Monte Carlo sampling!)

10: Convert the count of each sample value into probability and plot.

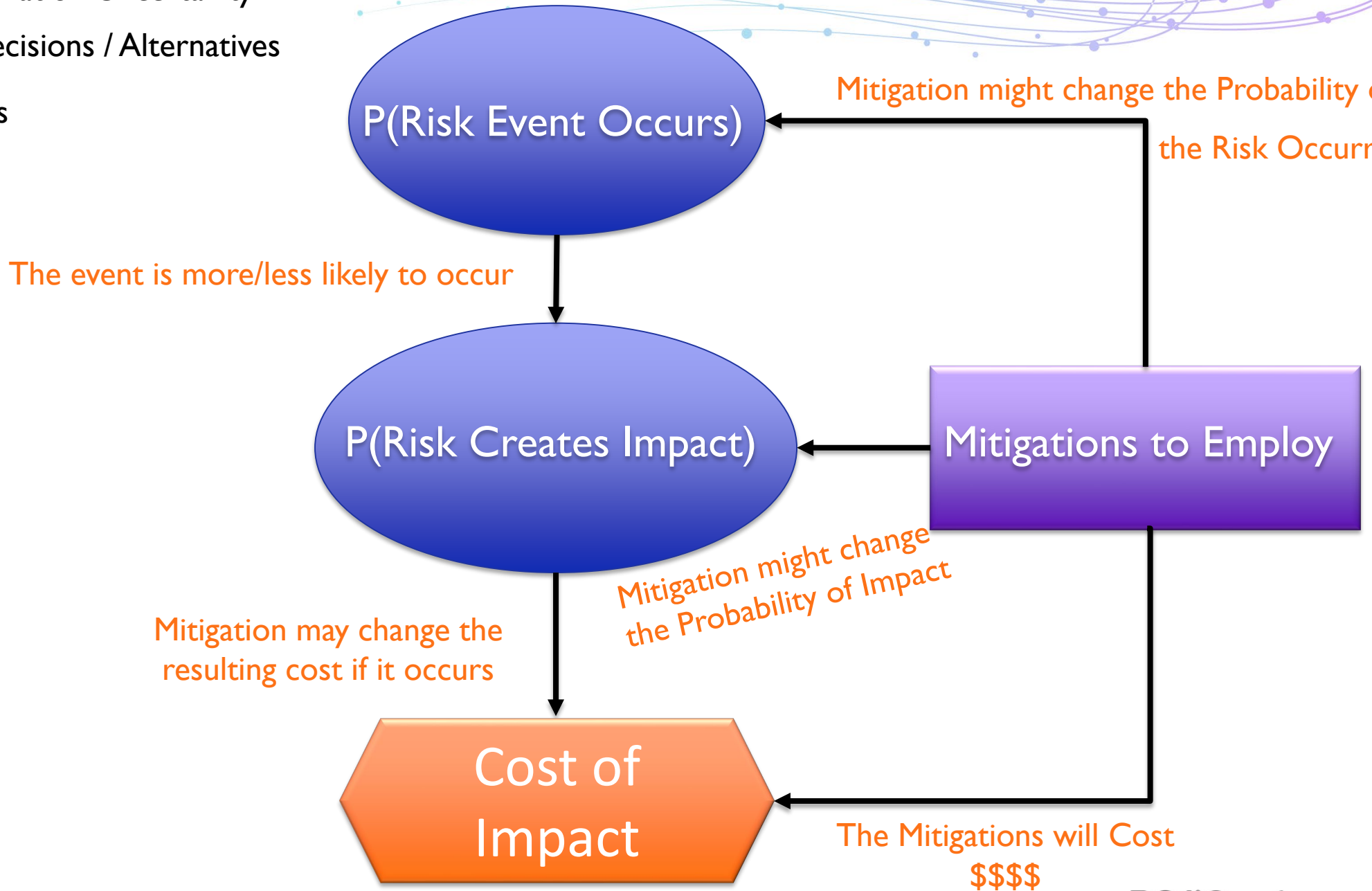
- Circles: Information Uncertainty
- Hexes: Values



- Circles: Information Uncertainty
- Rectangle: Decisions / Alternatives
- Hexes: Values



- Circles: Information Uncertainty
- Rectangle: Decisions / Alternatives
- Hexes: Values



Building a curve for Loss Exceedance

1: Identify your ~~organization's Risk Register Items.~~ **mitigations.**

2: Assess the probability of occurrence/impact for each Item **with mitigations.**

3: Assess the probability of various loss levels given the Item occurs **+ mitigations.**

4: Calculate the posterior probability loss distribution for each item.

5: Convert the previous to a cumulative distribution function (CDF) of loss.

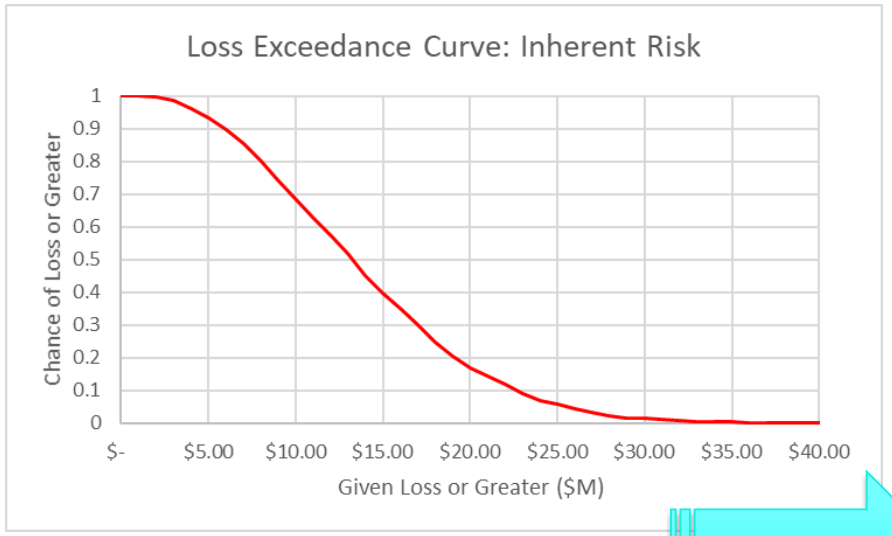
6: Repeat 2-5 for every Risk Register Item.

7: Sample the CDFs to generate sample losses.

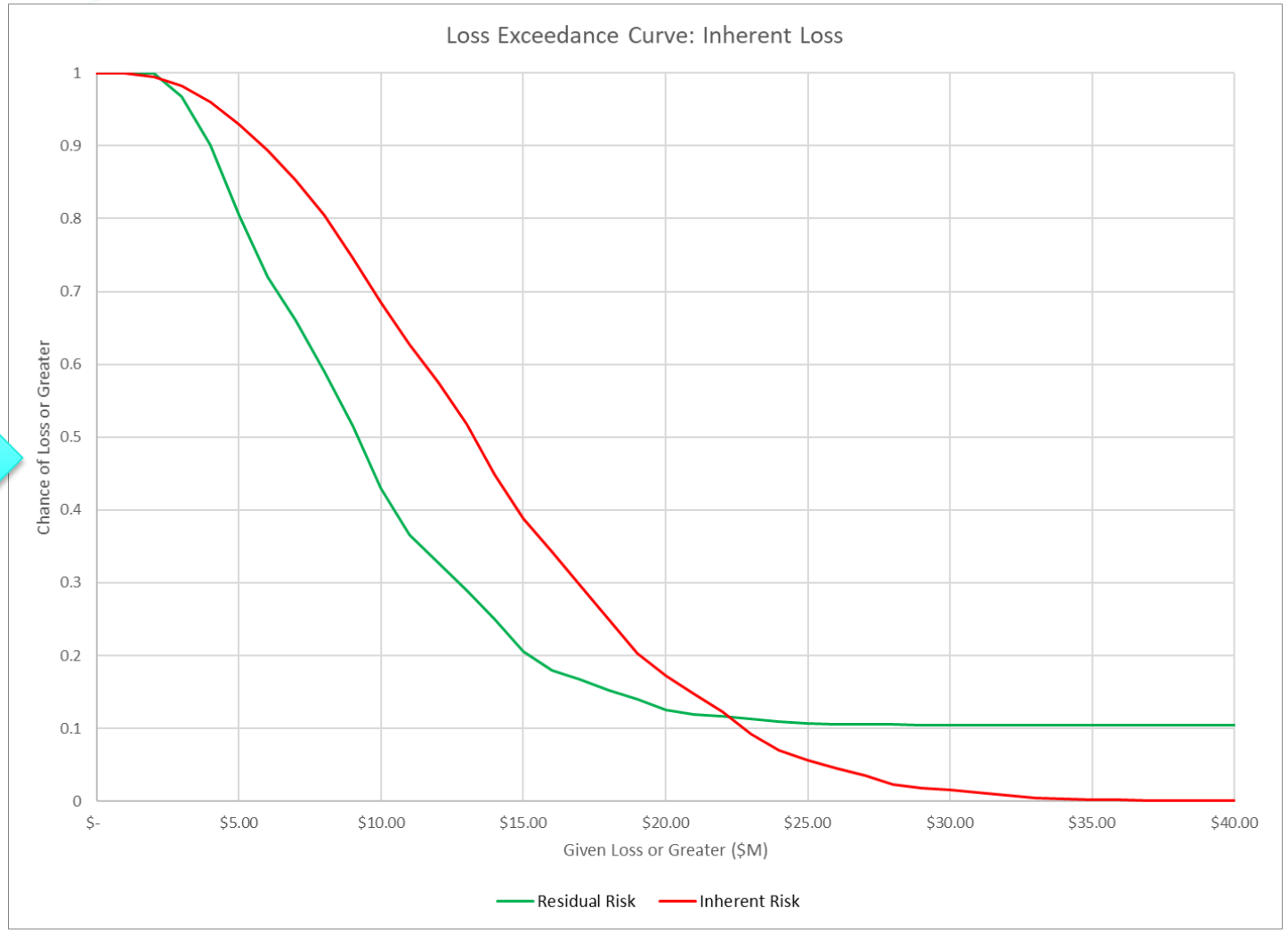
8: Add each of the Item's sampled losses => total loss for the sample.

9: Repeat 7-8 a couple 100,000's times (this is Monte Carlo sampling!)

10: Convert the count of each sample value into probability and plot.


Loss Exceedance Curve: Inherent Risk
Chance of Loss or Greater
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
$-
$5.00
$10.00
$15.00
$20.00
$25.00
$30.00
$35.00
$40.00
Given Loss or Greater ($M)


Loss Exceedance Curve: Residual Loss
Chance of Loss or Greater
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
$-
$5.00
$10.00
$15.00
$20.00
$25.00
$30.00
$35.00
$40.00
Given Loss or Greater ($M)


Loss Exceedance Curve: Inherent Loss
Chance of Loss or Greater
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
$-
$5.00
$10.00
$15.00
$20.00
$25.00
$30.00
$35.00
$40.00
Given Loss or Greater ($M)
Residual Risk
Inherent Risk


he E

RSAConference2019

What We Talked about

What We Talked About

Books that are important on this subject.

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

A history of "**Bayes**" and "**Monte Carlo**."

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

A history of "**Bayes**" and "**Monte Carlo**."

How to think about "**Superforecasting**."

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

A history of "**Bayes**" and "**Monte Carlo**."

How to think about "**Superforecasting**."

Why "**Latency Curves**" are better than Heat Maps.

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

A history of "**Bayes**" and "**Monte Carlo**."

How to think about "**Superforecasting**."

Why "**Latency Curves**" are better than Heat Maps.

Getting ready for the board.

What We Talked About

Books that are important on this subject.

"**Heat Maps**" are bad science.

The **probability theory** that you thought you learned in college is wrong.

A history of "**Bayes**" and "**Monte Carlo**."

How to think about "**Superforecasting**."

Why "**Latency Curves**" are better than Heat Maps.

Getting ready for the board.

How to build "**Latency Curves**."

RSAConference2019

Homework

Homework

Next Week

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Six Months

Re-write your risk register items to accommodate the Superforecasting idea.

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Six Months

Re-write your risk register items to accommodate the Superforecasting idea.

Read one of the three key books.

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Six Months

Re-write your risk register items to accommodate the Superforecasting idea.

Read one of the three key books.

Build Proof-of-Concept Latency Curves in Excel for your Risk Register items.

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Six Months

Re-write your risk register items to accommodate the Superforecasting idea.

Read one of the three key books.

Build Proof-of-Concept Latency Curves in Excel for your Risk Register items.

This Year

Socialize the Superforecasting method with your own business leaders.

Homework

Next Week

Download and read the White Paper & Slides

https://paloaltonetworks.box.com/s/yncxz78q66mh66x9rohn79soe255fxk7

Send a twitter note to @racebannon99, I will send the link.

Visit the Canon Website and read a book from the Hall of Fame of List

https://cybercanon.paloaltonetworks.com/

Six Months

Re-write your risk register items to accommodate the Superforecasting idea.

Read one of the three key books.

Build Proof-of-Concept Latency Curves in Excel for your Risk Register items.

This Year

Socialize the Superforecasting method with your own business leaders.

Send feedback to me and Dave


No – Really This Time

Contact Info

Rick Howard: CSO Palo Alto Networks

Email: rhoward@paloaltonetworks.com

Twitter: @raceBannon99

CYBERSECURITY CANON

https://cybercanon.paloaltonetworks.com/

David Caswell: Computer Science Head, USAFA

Email: david.caswell@edu.usafa.edu

paloalto NETWORKS