FAIR CONFERENCE 2019

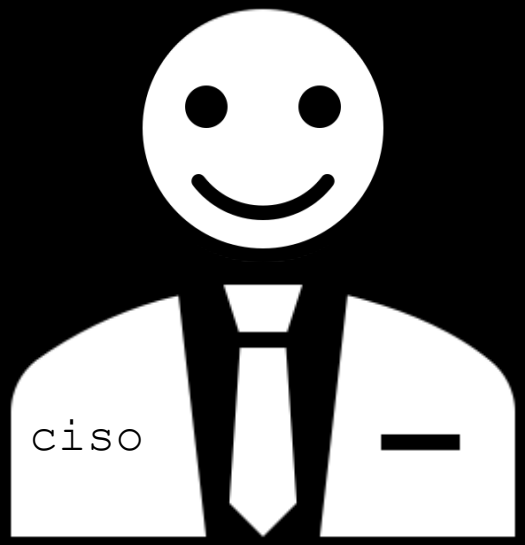
Using FAIR to take the Headache out of considering Cyber Insurance for your Business

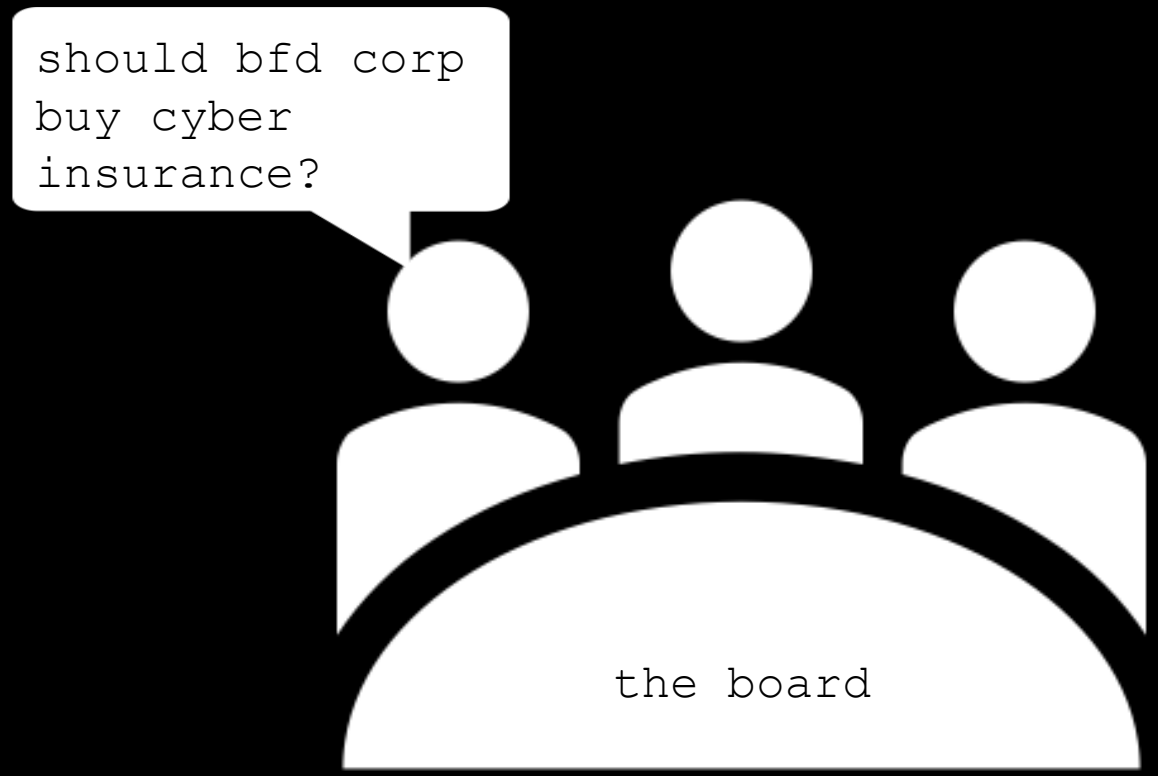
JEREMY ALEXANDER

Sr. Risk Expert, Information Security
Decision Science
Walmart

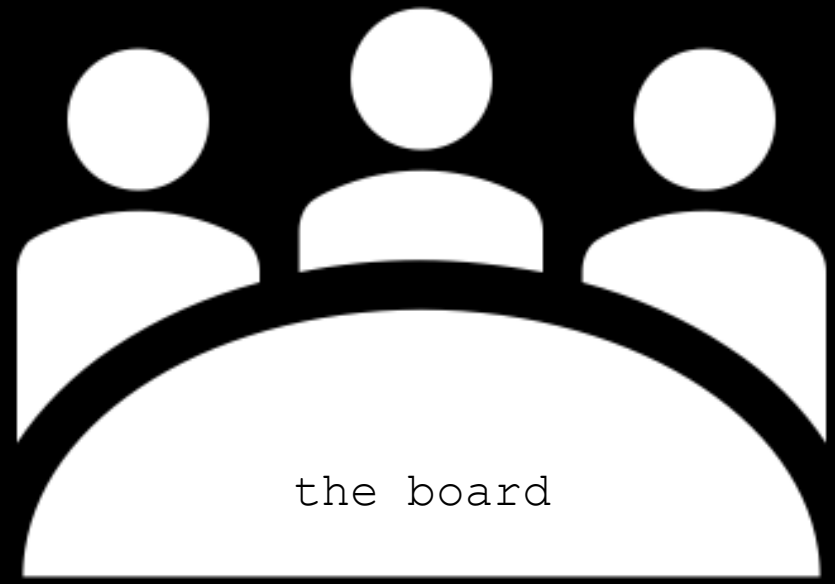
disclaimer

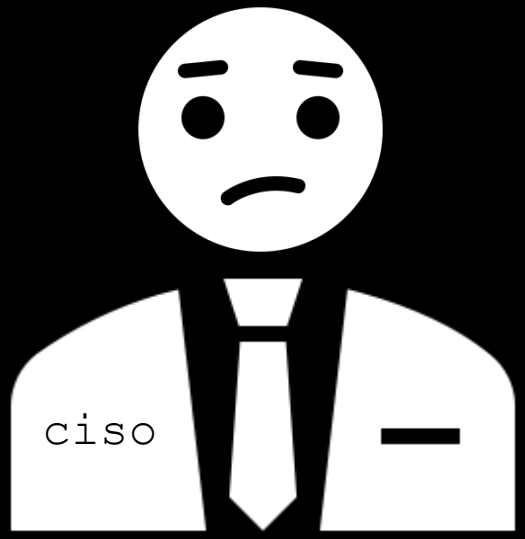
this is a work of fiction. names, characters, businesses, places, events, locales, and incidents are either the products of the author’s imagination or used in a fictitious manner (except for mathematical formulae). any resemblance to actual persons, living or dead, or actual events is purely coincidental

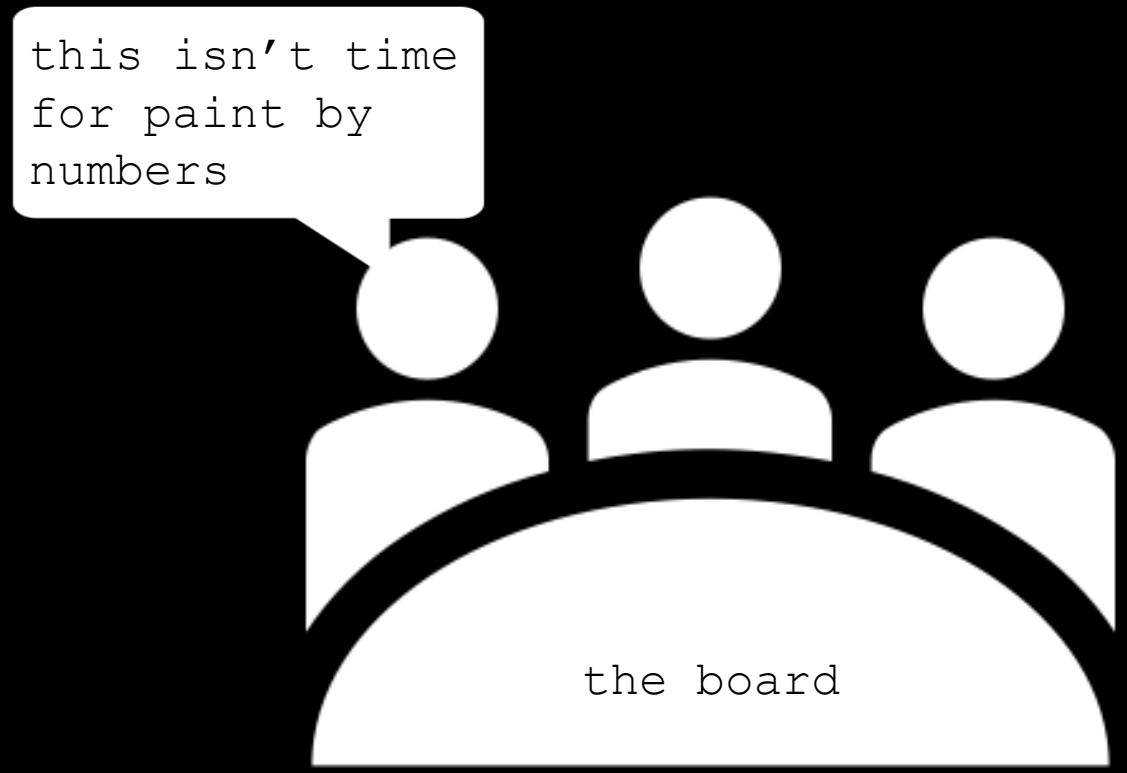

ciso

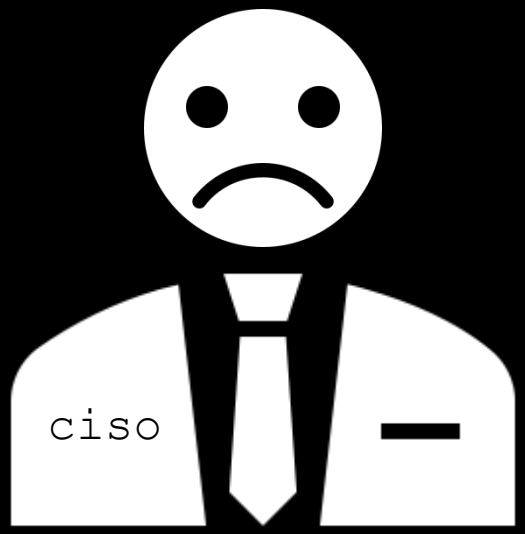

should bfd corp buy cyber insurance?
the board

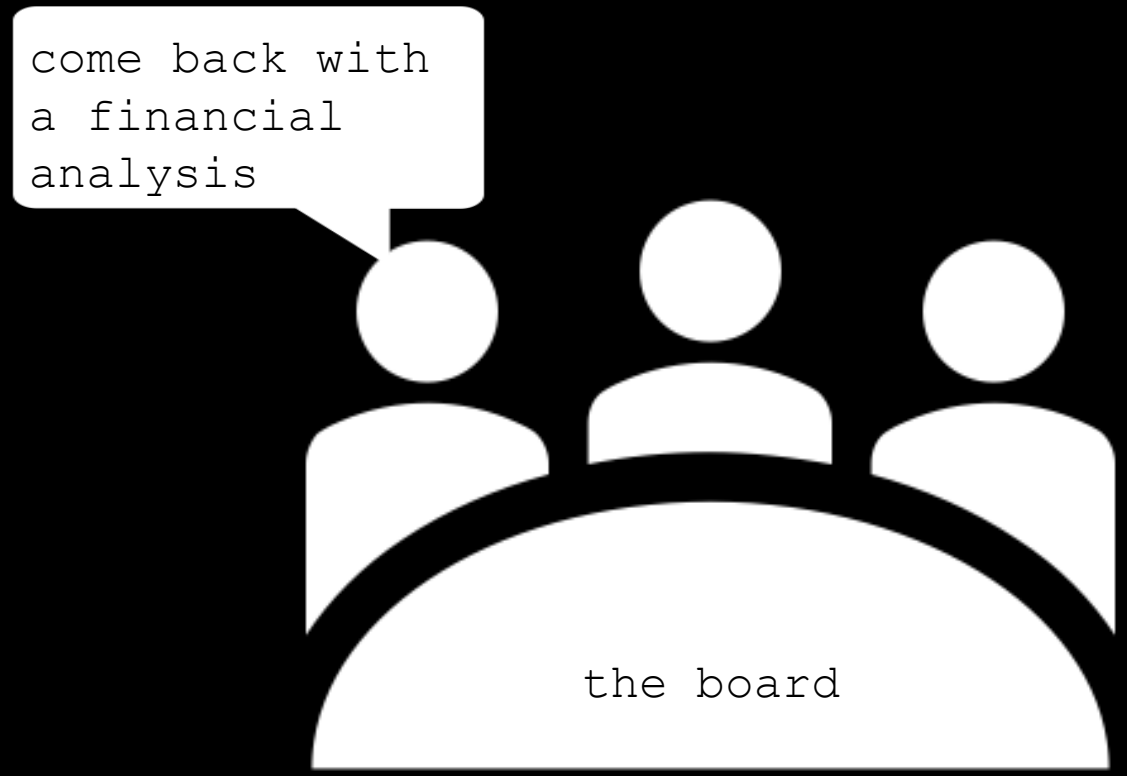

well, the threat meter is red sir…
ciso

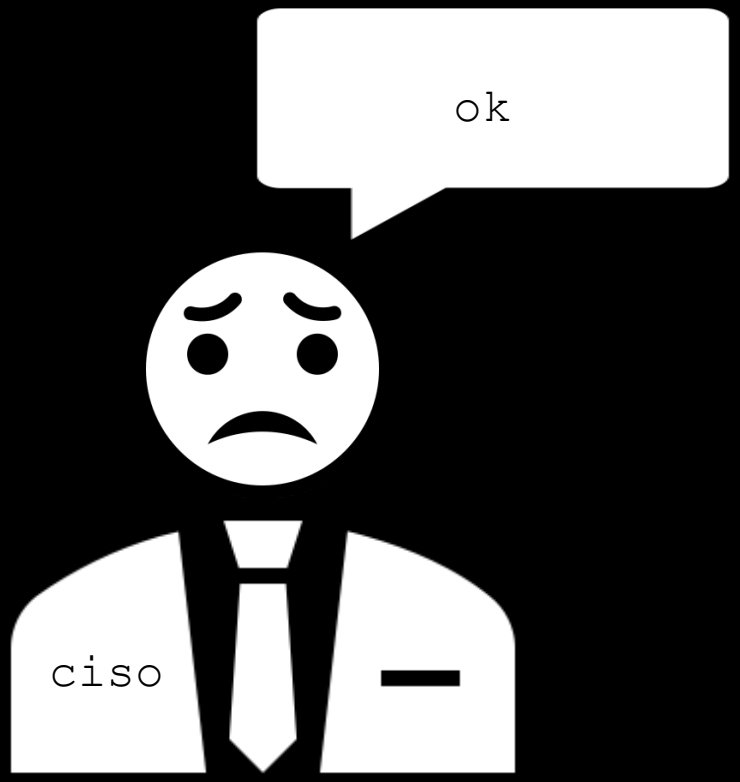

the board

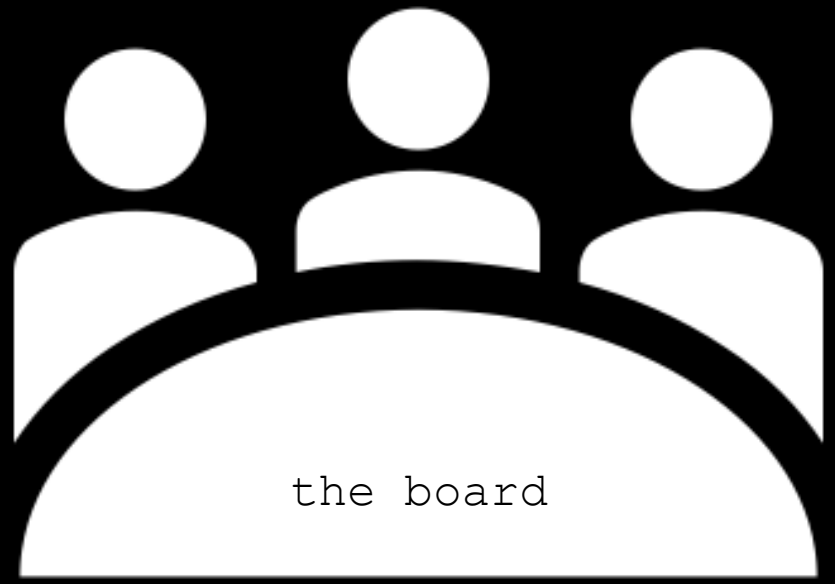

ciso


this isn’t time for paint by numbers
the board

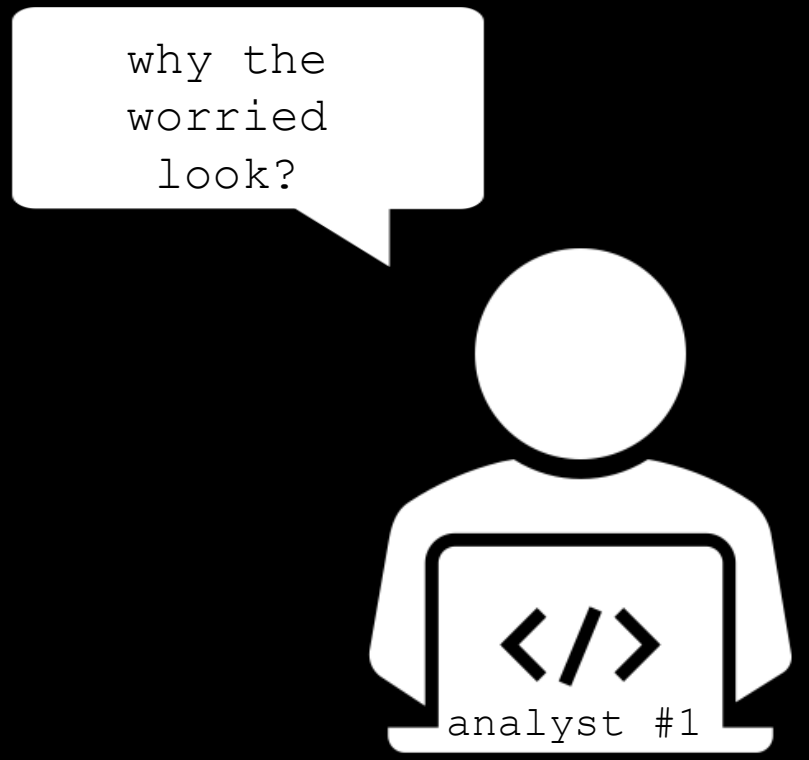

ciso


come back with a financial analysis
the board


ok
ciso


the board

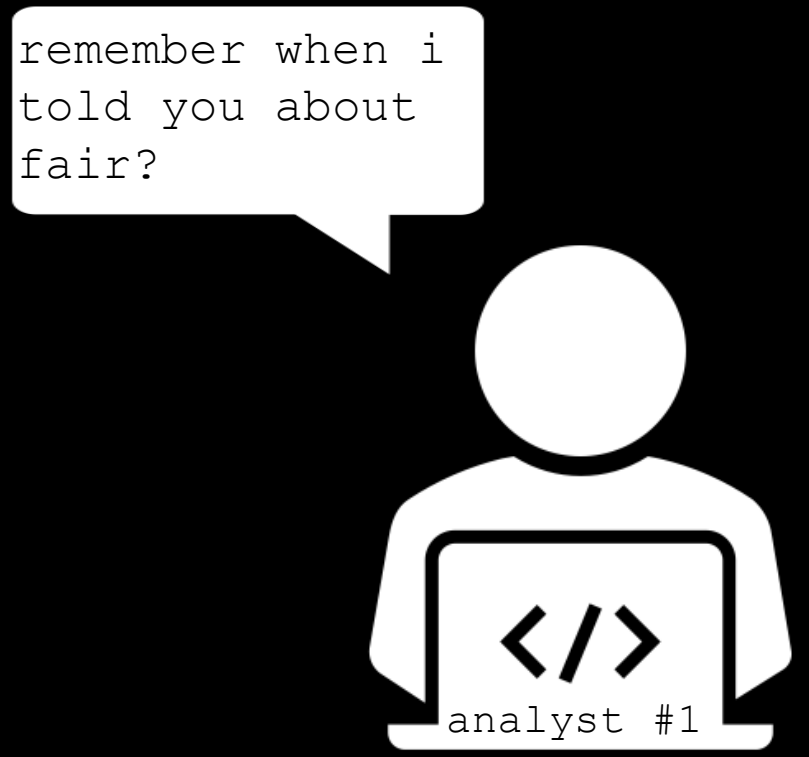

ciso

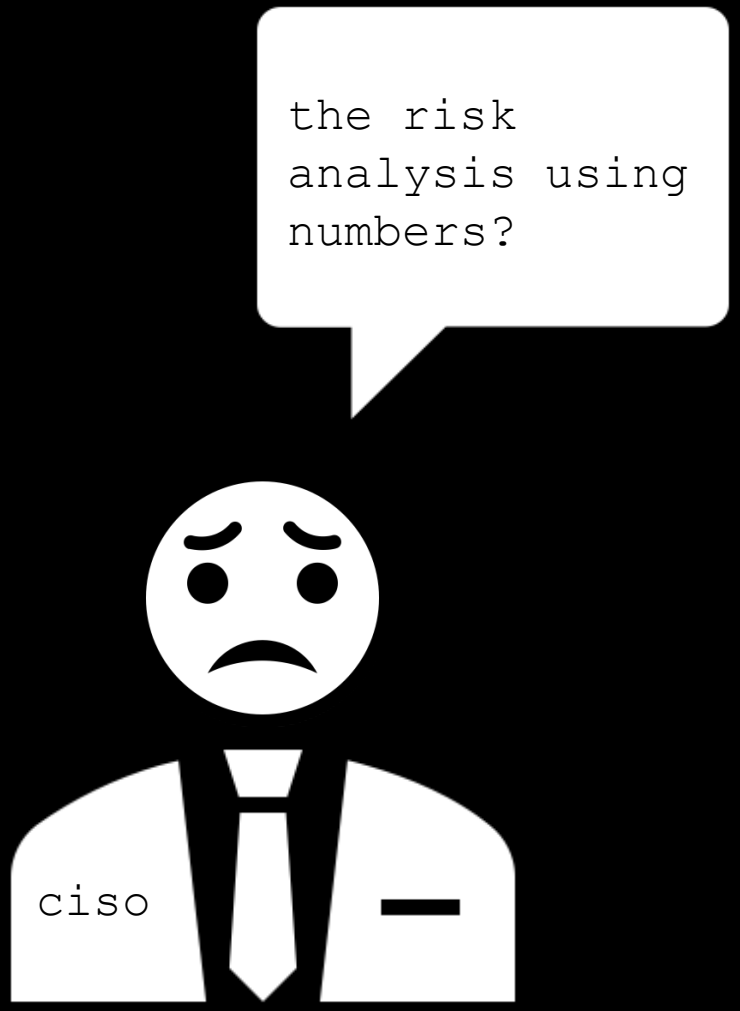

why the worried look?
analyst #1

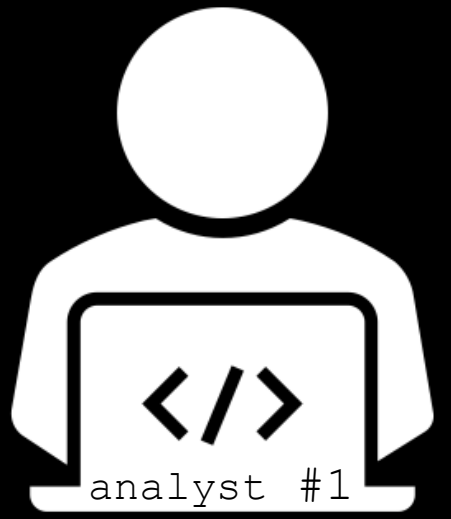

i need to make a financially-based recommendation to the board for or against purchasing cyber insurance
ciso

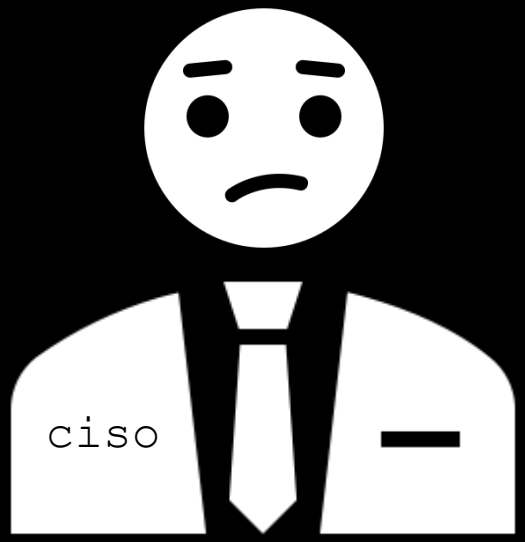

analyst #1

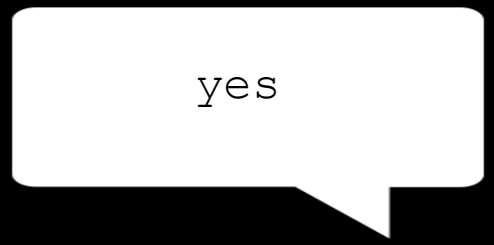

ciso


remember when i told you about fair?
analyst #1

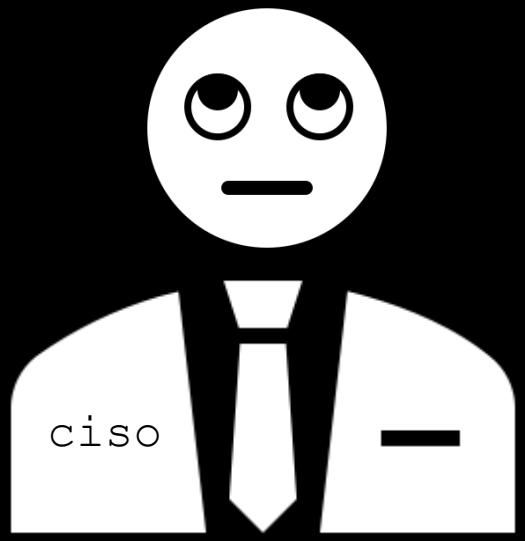

the risk analysis using numbers?
ciso

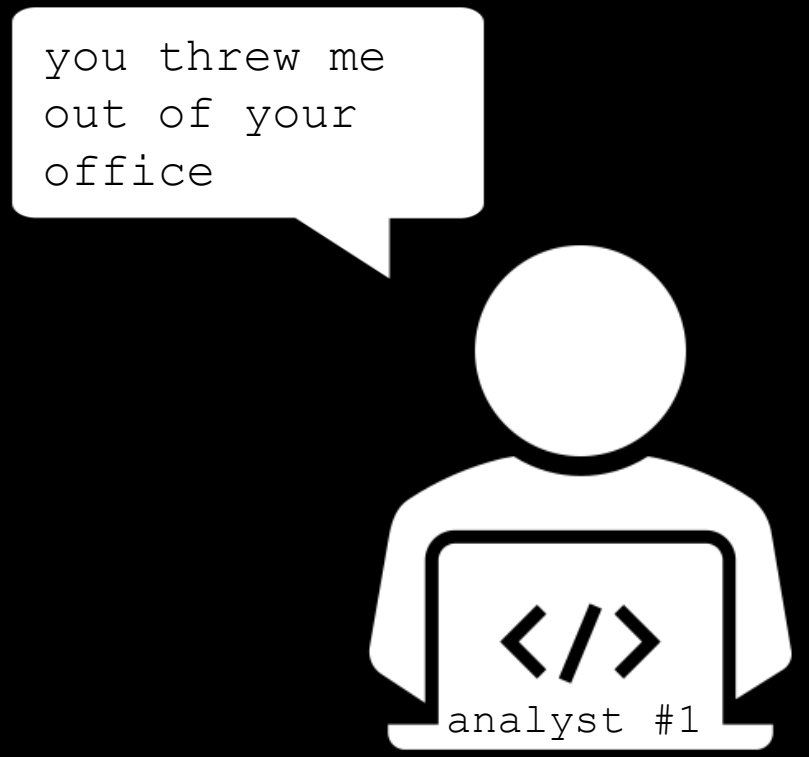

analyst #1


ciso


yes

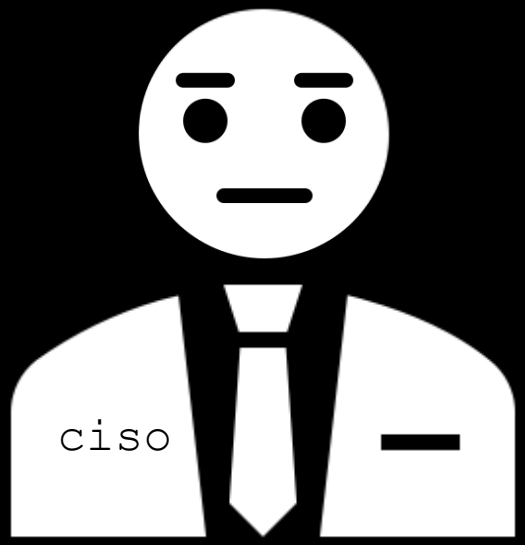

analyst #1

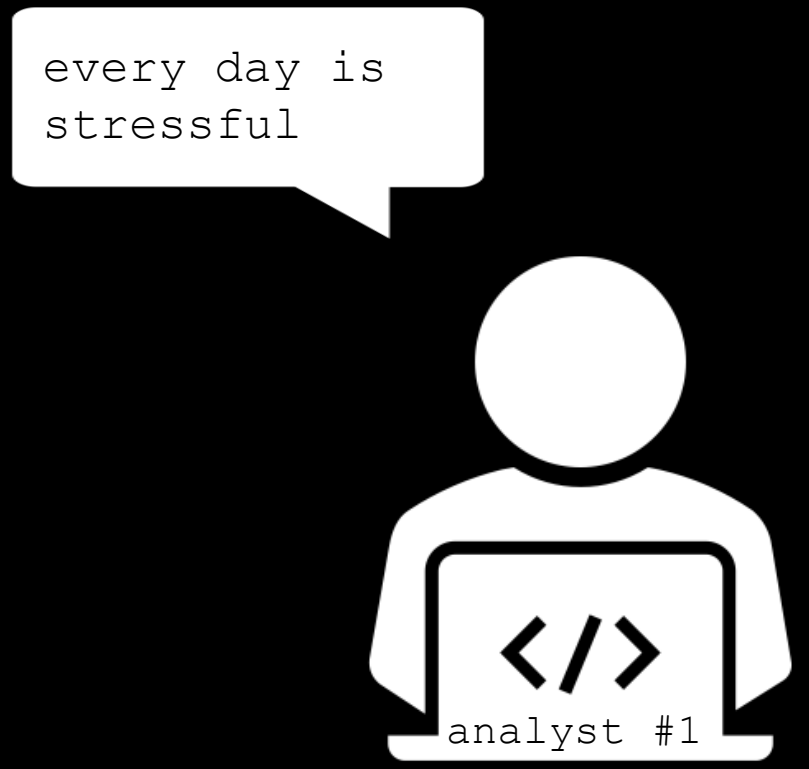

ciso


you threw me out of your office
analyst #1


it was a stressful day
ciso

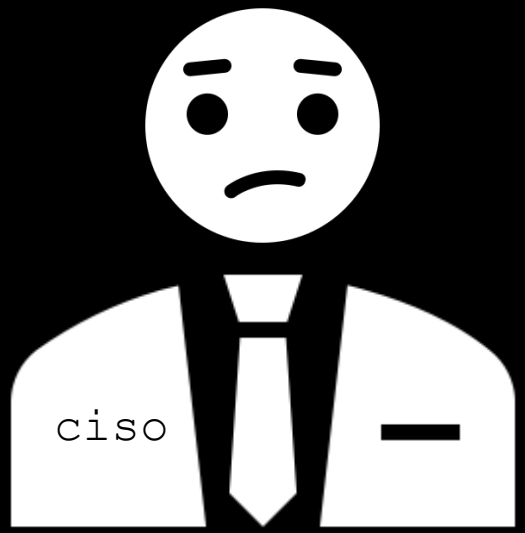

analyst #1


ciso

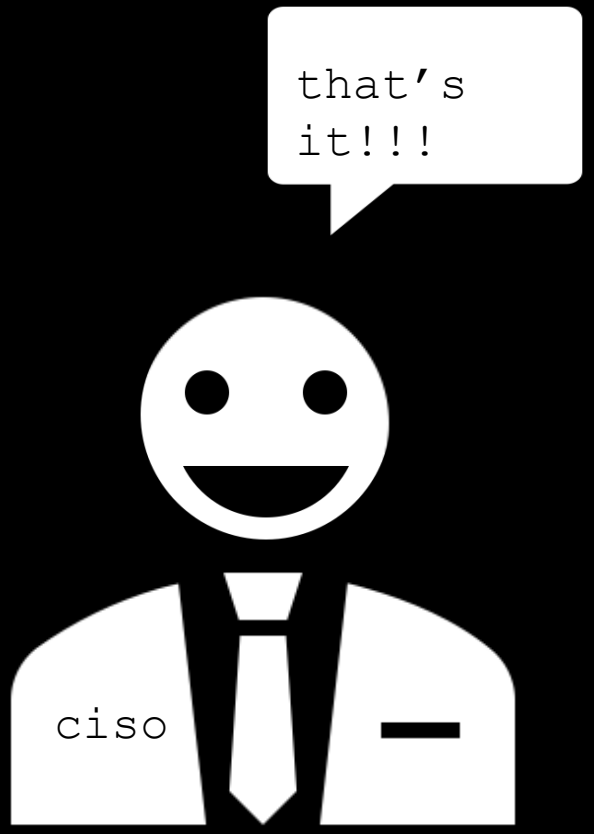

every day is stressful
analyst #1


i remember, so what does my problem have to do with fair?
ciso


analyst #1

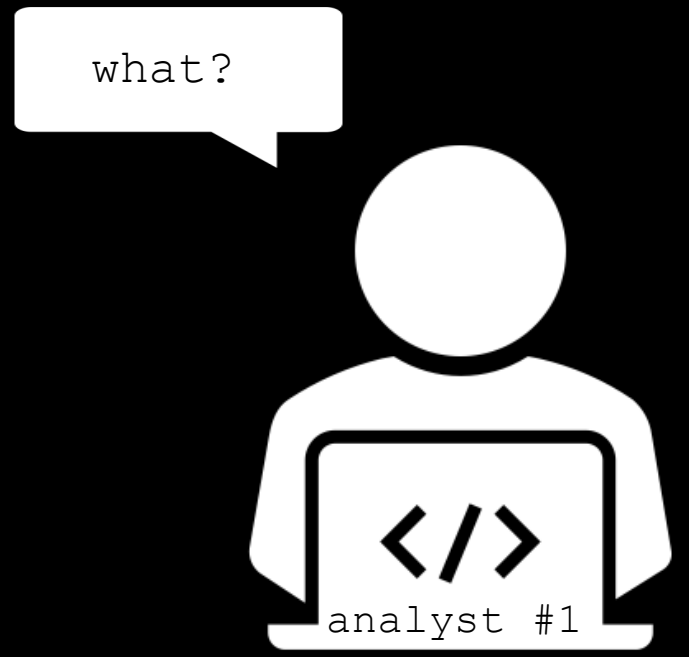

ciso

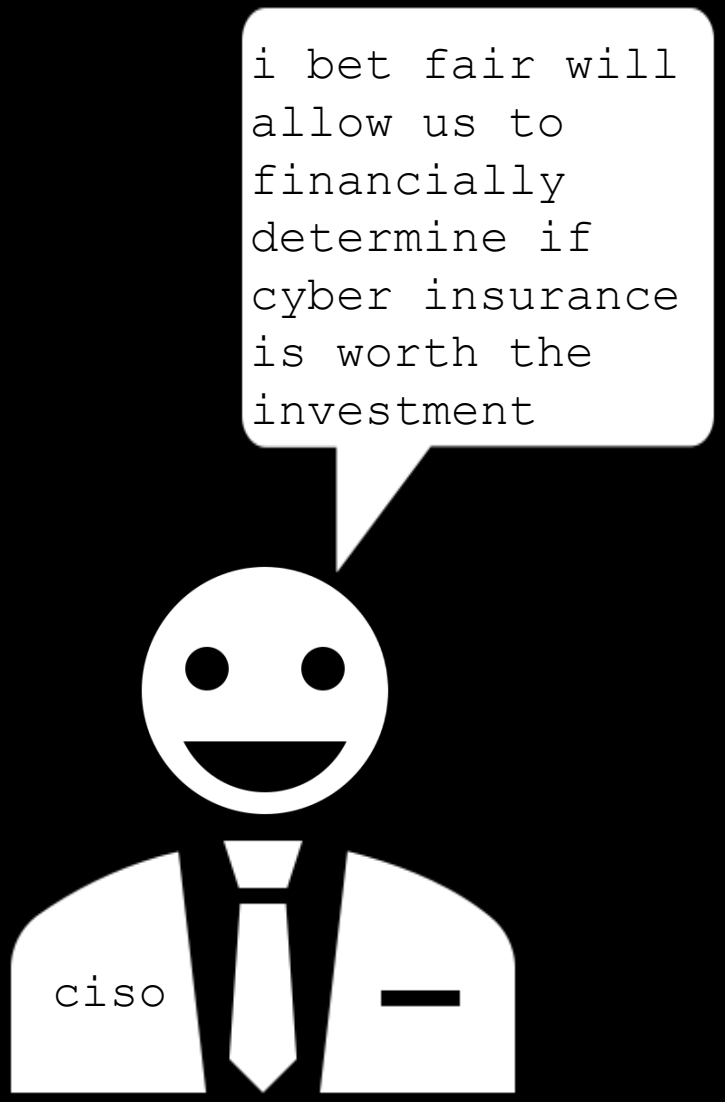

if risk is quantified in dollars, and if financial recommendations are usually made with dollars in mind…
analyst #1


that’s
it!!!
ciso

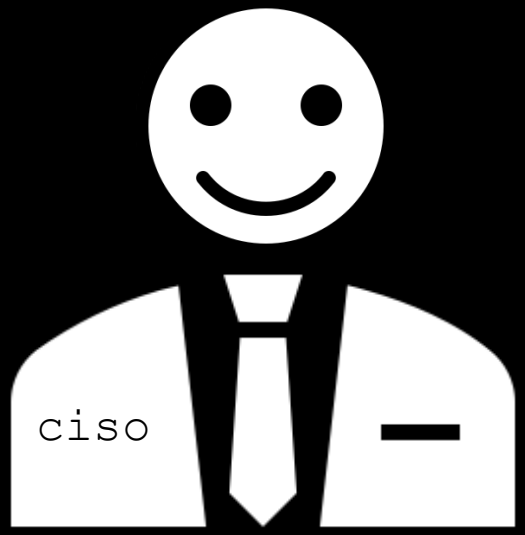

analyst #1

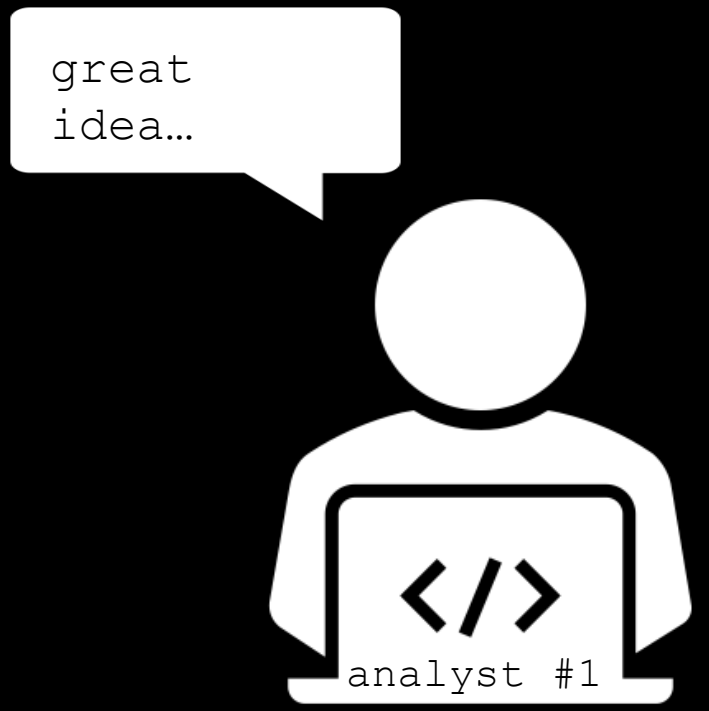

ciso


what?
analyst #1


i bet fair will allow us to financially determine if cyber insurance is worth the investment
ciso

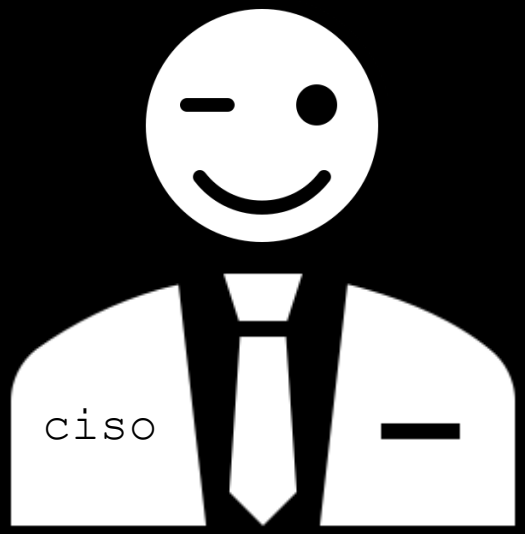

analyst #1


ciso


great
idea…
analyst #1


really???
thanks!
ok, get to
work
ciso


analyst #1


ciso


will
do
analyst #1


choose your
scenarios wisely…

$

open log file bucket

$$$

big breach

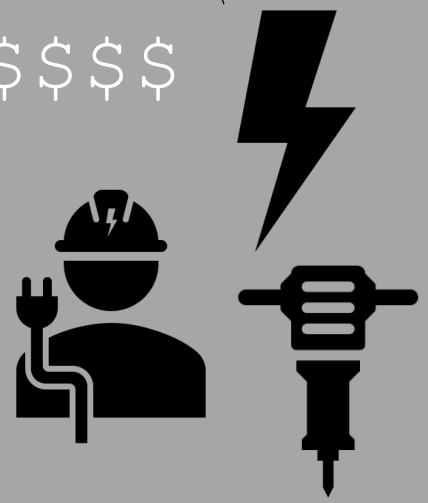
$$$$$

armageddon

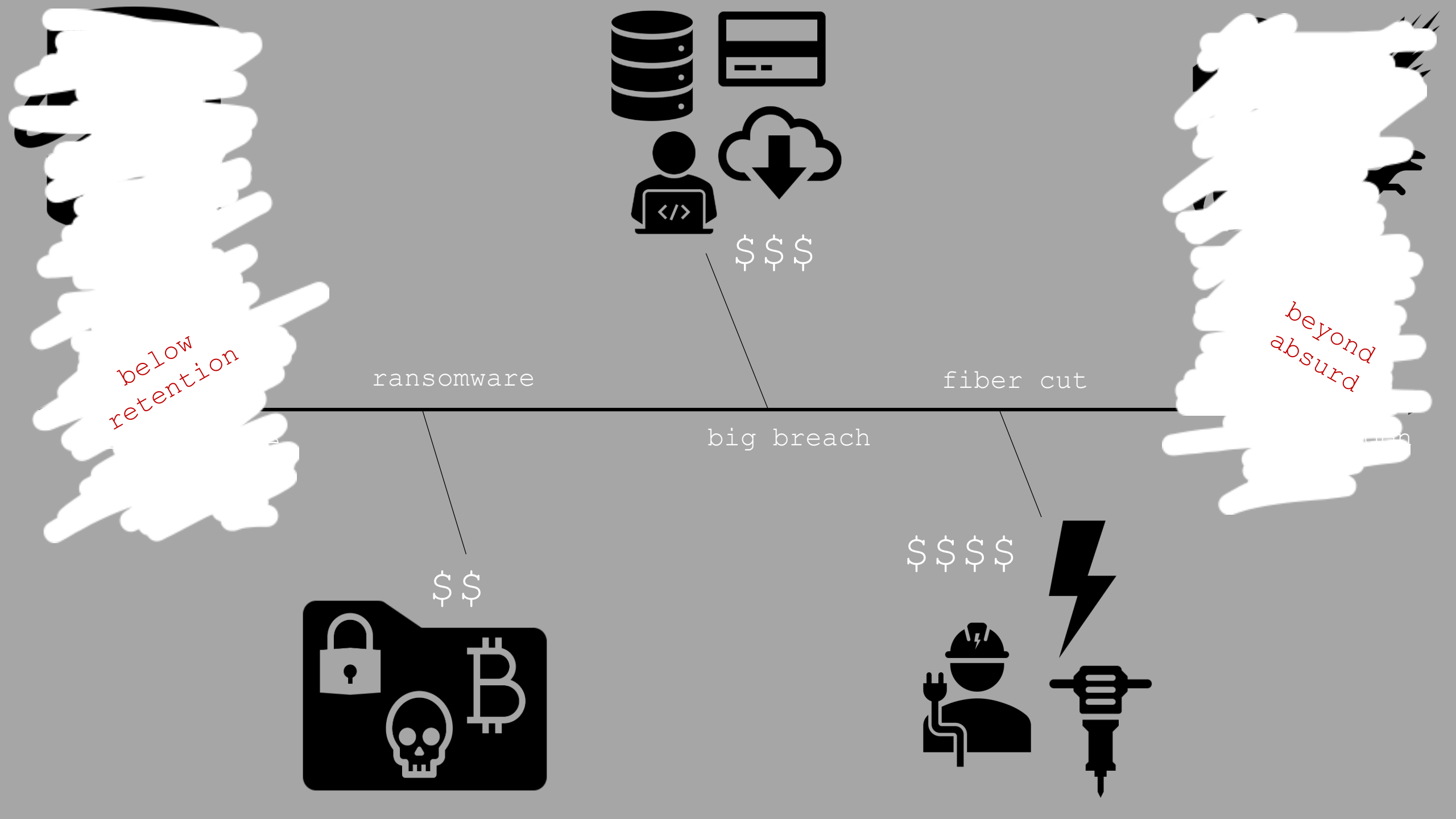
ransomware

$$

fiber cut

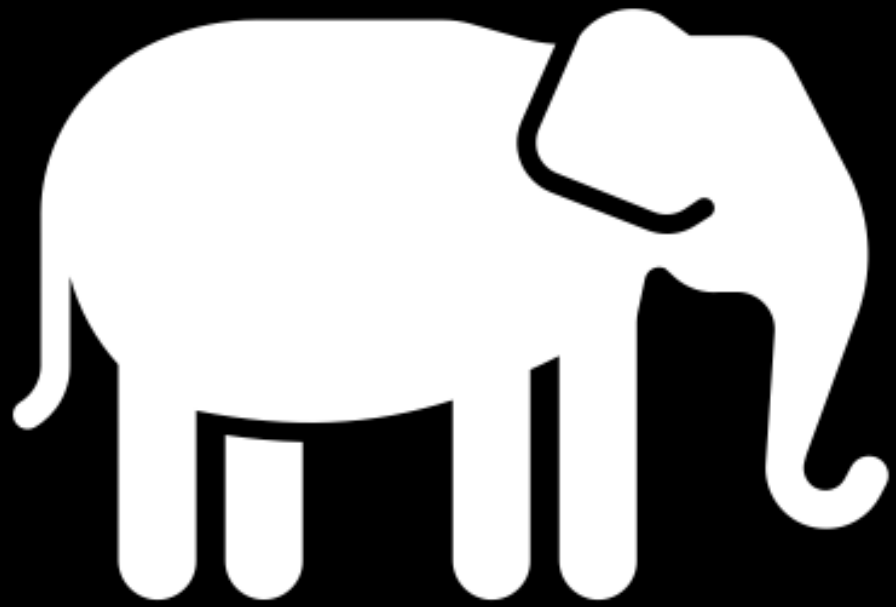


$$$$


below retention
ransomware
big breach
fiber cut
beyond absurd
$$$
$$
$$$$

is it large enough?
(policy retention)

is it probable
enough? (no
asteroid strikes)



loss magnitude

about 40 million cards lost

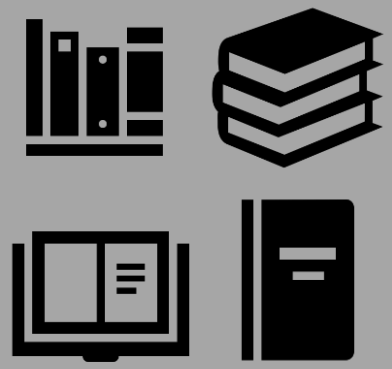
cost $200 – $300 million

$5.00 - $7.50 per record

how many sensitive records might bfd corp lose?

25 million records
x
$6.00

$150
million



sasha romanosky
every 10% increase in company revenues corresponded to a 1.3% increase in cost of incident

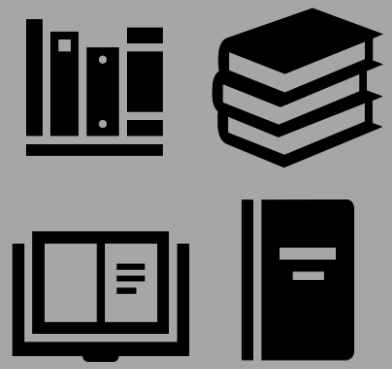
extrapolate for the bfd corporation

bullseye company
annual revenue $75 billion

bfd corporation
annual revenue $20 billion

$209 million

sasha romanosky. (2016) examining the costs and causes of cyber incidents. journal of cybersecurity, 2: 121-135.



sasha romanosky
every 10% increase in compromised records corresponded to a 2.9% increase in cost of incident

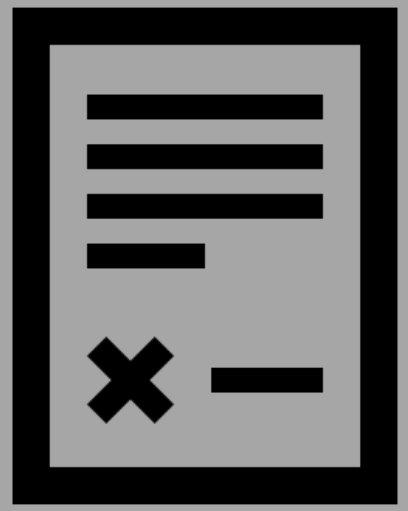
extrapolate for the bfd corporation

bullseye company
records taken 40 million

bfd corporation
records at stake 25 million

$217 million

sasha romanosky. (2016) examining the costs and causes of cyber incidents. journal of cybersecurity, 2: 121-135.

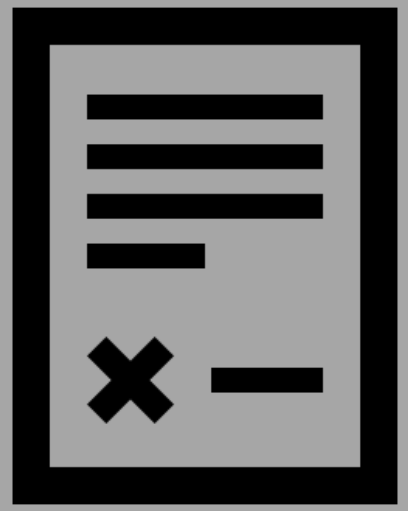


the policy considered is capped at coverage of $215 million per event

your highest estimated single loss magnitude is a little higher than this

coverage appears sufficient and for simplicity consider a $209m loss

$150 million $209 million $217 million



the policy capped at $215 million per event

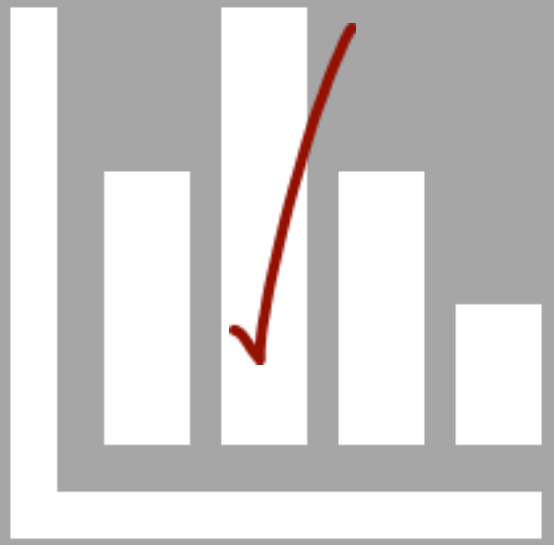
has a $40 million retention

and premiums are $4 million

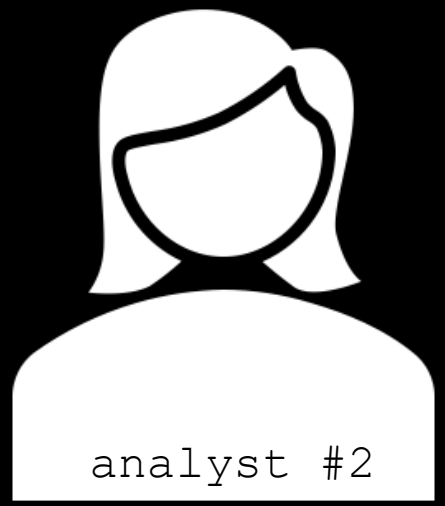

frequency

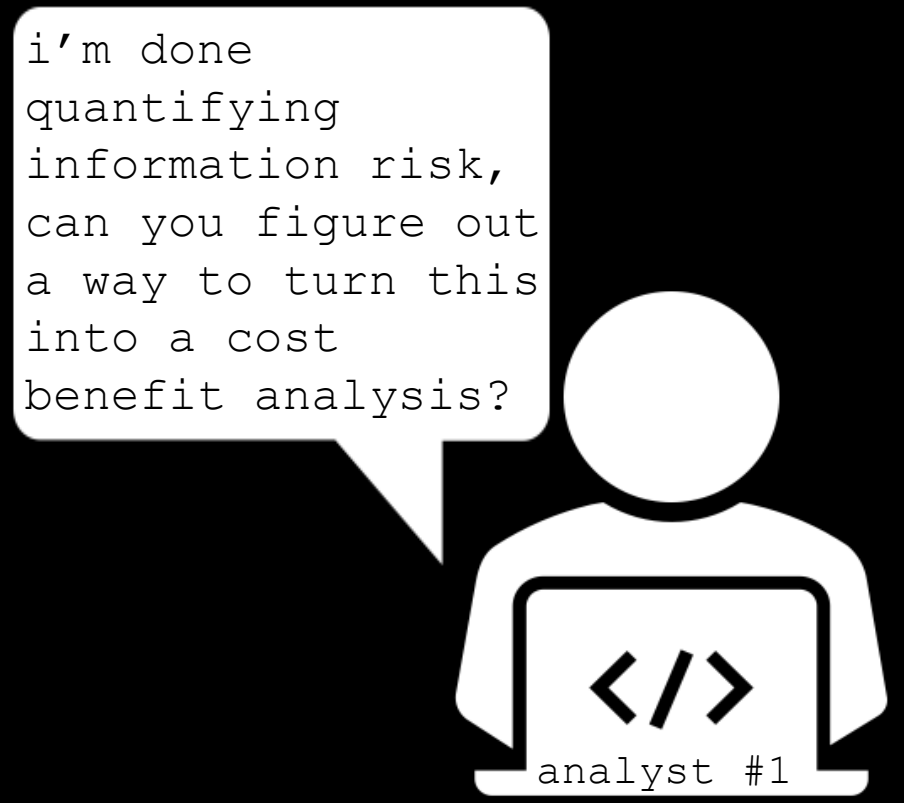
instead of settling on one reasonable estimate like single loss magnitude

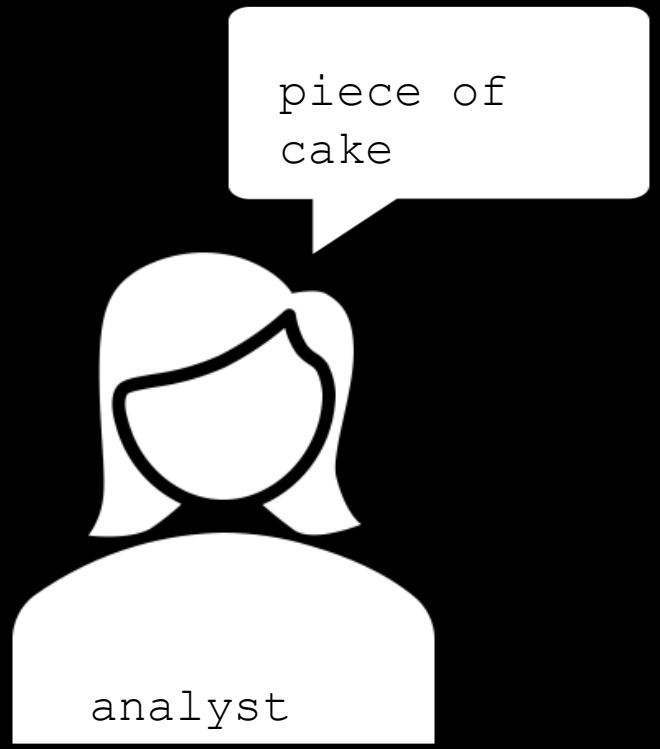
allow for a range of possible frequencies with most likely



1/10 years 1/20 years 1/30 years

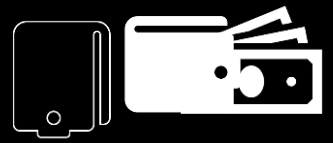

analyst #2


i’m done quantifying information risk, can you figure out a way to turn this into a cost benefit analysis?
analyst #1


piece of cake
analyst


analyst #1

cost benefit



consider a cost benefit analysis

over the next 20 years

comparing risk acceptance versus transference

the value of invested avoided premiums over a 20 year period is given by

20 year period

$4 million annual premium

geometric series

$$\$288M = \$4M\,\frac{1-1.12^{20}}{1-1.12} = \sum_{n=0}^{19} (\$4M)\,1.12^{n}$$

12% annual return rate

the cost to achieve this value over the next 20 years is given by

avoided premiums

1 event in 20 years

20 year period

most likely single loss magnitude

$$\$289M = \$80M + (.05)(20)(209)$$

the cost for one major event every 30 years is given by

avoided premiums

1 event in 30 years

20 year period

most likely single loss magnitude

$$\$218M = \$80M + (.033)(20)(209)$$

the cost for one major event every 10 years is given by

avoided premiums

1 event in 10 years

20 year period

most likely single loss magnitude

$$\$498M = \$80M + (.1)(20)(209)$$

the most likely annualized rate of return is given by

$$0.0\% = \left((\$288M - \$289M)\right)/\$289M/20$$

value

cost

20 year period

the 1 in 30 annualized rate of return is given by

$$+1.6\% = \big((\$288M - \$218M)\big)/\$218M/20$$

value

cost

20 year period

the 1 in 10 annualized rate of return is given by

$$-2.1\% = \big((\$288M - \$498M)\big)/\$498M/20$$

value

cost

20 year period

for self-insurance annual rate of return we have

min: -2.1% for one major event every 10 years

most likely: 0.0% for one major event every 20 years

max: +1.6% for one major event every 30 years

the most likely value from transferring risk over the next 20 years is given by

1 event in 20 years

20 year period

$$\$209M = (.05)(20)(209)$$

most likely single loss magnitude

the value for 1 in 30 year frequency over the next 20 years is given by

1 event in 30 years

20 year period

$$\$138M = (.033)(20)(209)$$

most likely single loss magnitude

the value for 1 in 10 year frequency over the next 20 years is given by

1 event in 10 years

20 year period

most likely single loss magnitude

$$\$418M = (.10)(20)(209)$$

the most likely cost from transferring risk over the next 20 years is given by

1 event in 20 years

20 year period

premiums

$$\$120M = 80M + (.05)(20)(40M)$$

retention threshold

the 1 in 30 year cost from transferring risk over the next 20 years is given by

premiums

1 event in 30 years

20 year period

$$\$106M = 80M + (.033)(20)(40M)$$

retention threshold

the 1 in 10 year cost from transferring risk over the next 20 years is given by

premiums

1 event in 10 years

20 year period

$$\$160M = 80M + (.10)(20)(40M)$$

retention threshold

the most likely annualized rate of return is given by

$$+3.7\% = \big((\$209M - \$120M)\big)/\$120M/20$$

value

cost

20 year period

the 1 in 30 years annualized rate of return is given by

$$+1.5\% = \big((\$138M - \$106M)\big)/\$106M/20$$

value

cost

20 year period

the 1 in 10 years annualized rate of return is given by

$$+8.1\% = \big((\$418M - \$160M)\big)/\$160M/20$$

value

cost

20 year period

the transference annual rate of return we have

min: +1.5% for one major event every 10 years

most likely: +3.7% for one major event every 20 years

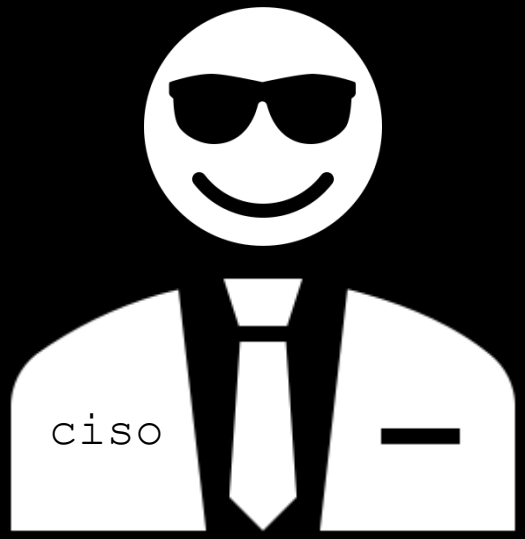
max: +8.1% for one major event every 30 years

option	min	most likely	max
self-insure	-2.1%	0.0%	+1.6%
transfer	+1.5%	+3.7%	+8.1%

transfer

epilogue

after the fair savvy risk analysts completed their work, our concerned ciso wowed the board of directors with a strong case justifying the purchase of cyber insurance, after which the board elected not to purchase, because they felt the budget dollars should go toward a more important project… finding a jet with more comfortable seats




wheeeeee!!!!

disclaimer

this is a work of fiction. names, characters, businesses, places, events, locales, and incidents are either the products of the author’s imagination or used in a fictitious manner (except for mathematical formulae). any resemblance to actual persons, living or dead, or actual events is purely coincidental