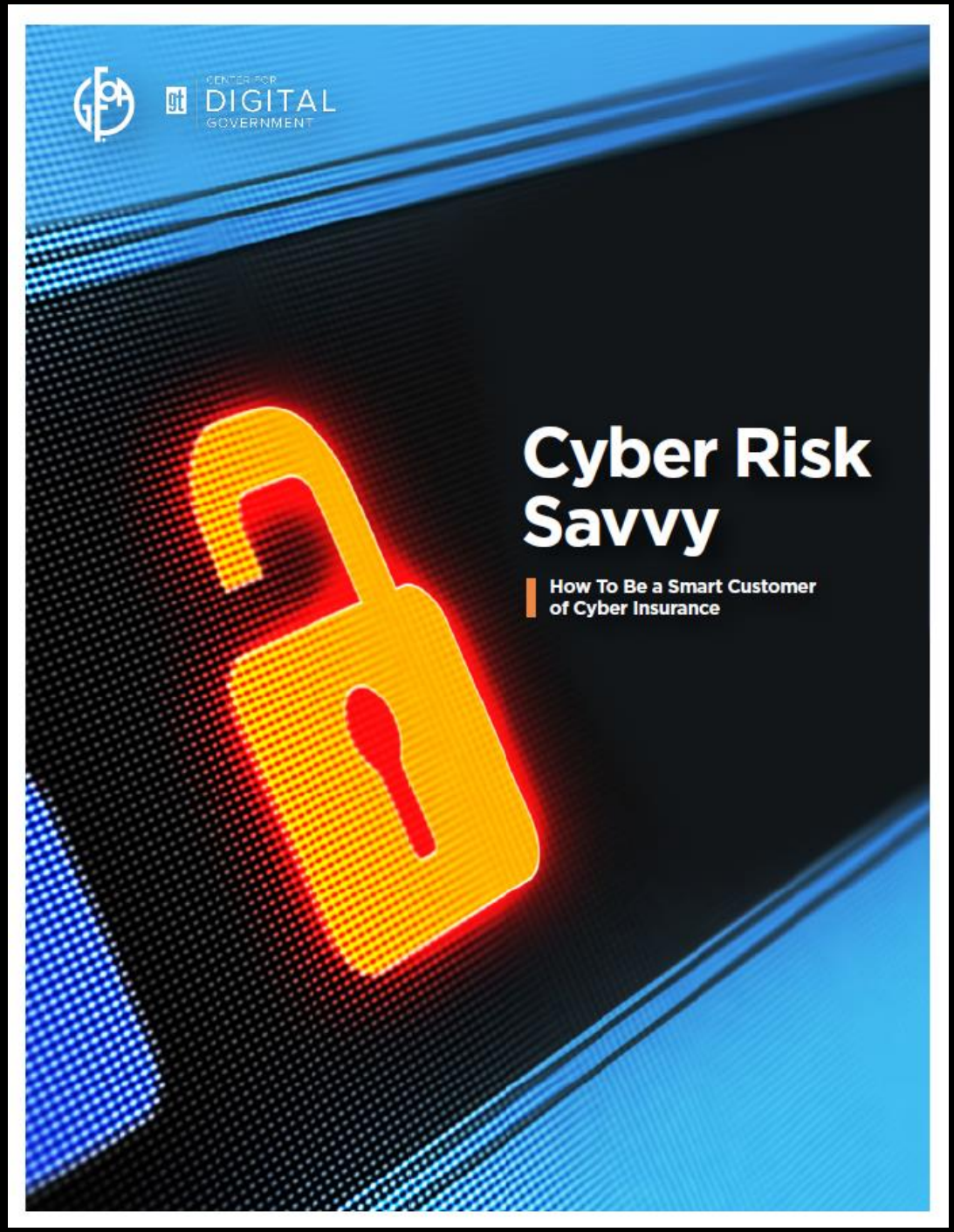
Cyber Risk Savvy: How to be a Smart Customer of Cyber Insurance



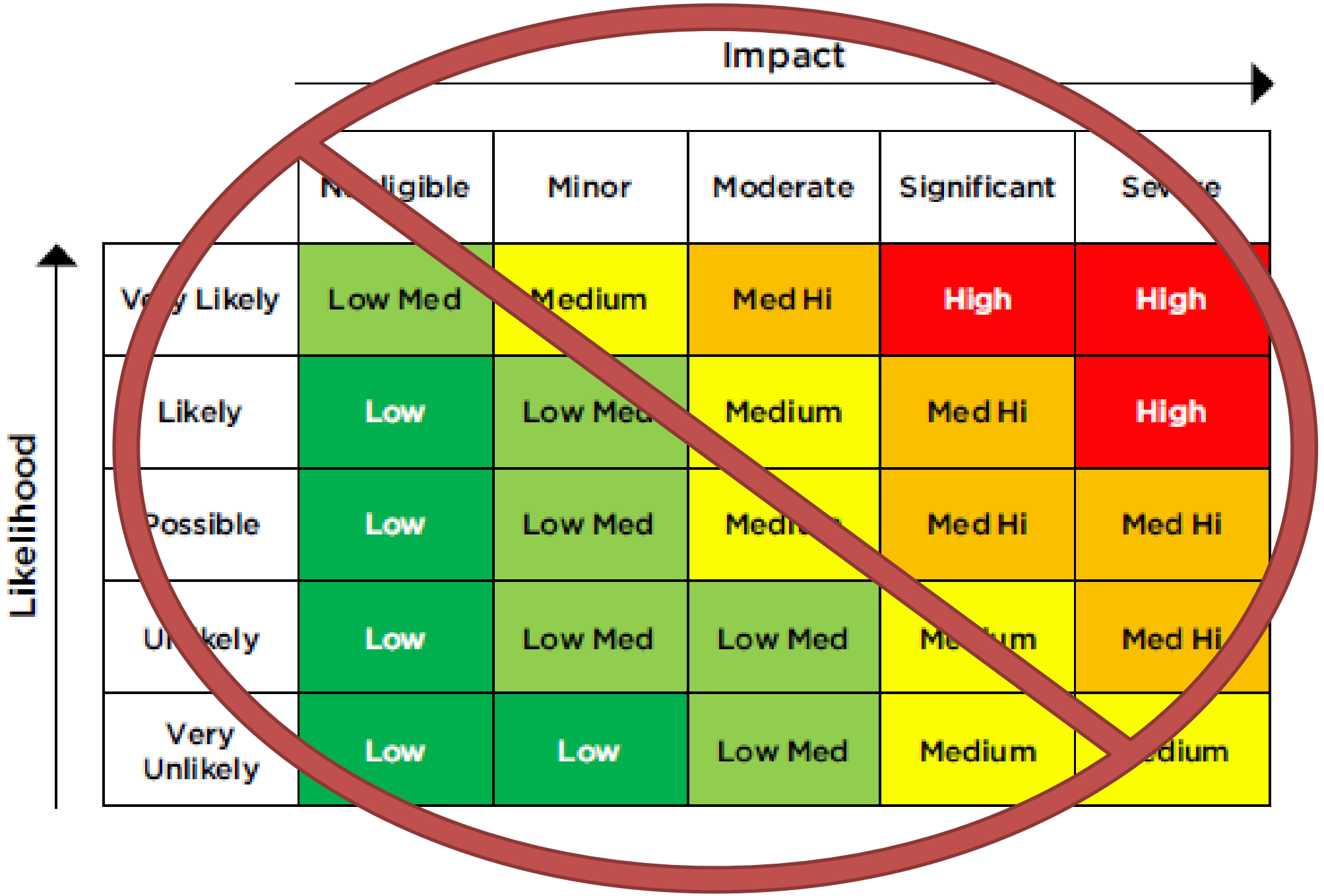
Four Step Process for Considering Cyber Insurance

Step 1 – Know the basics of your cybersecurity situation

Step 2 – Quantify your risk

Step 3 – Examine the potential of insurance

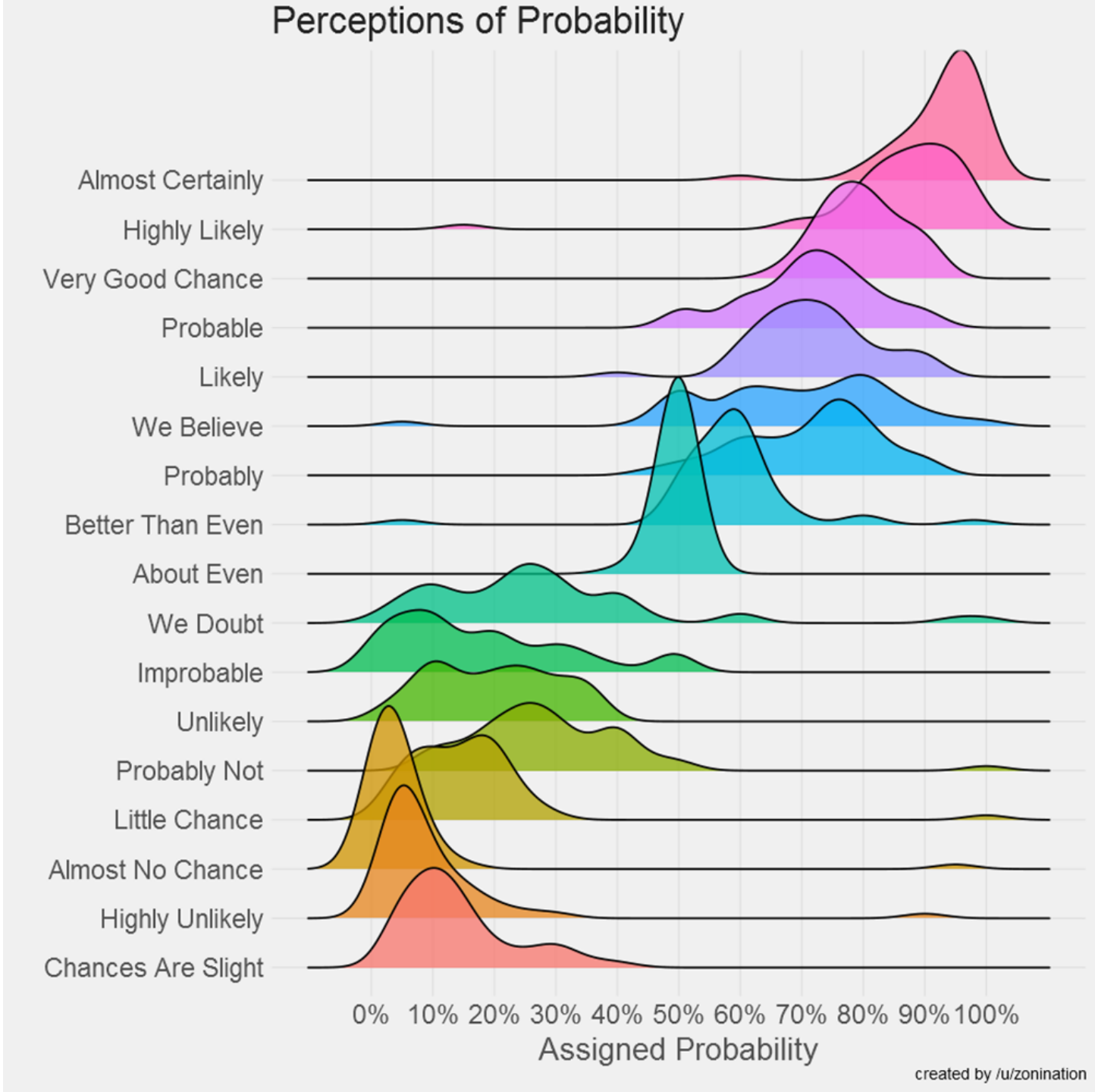
Step 4 – Periodically re-assess


Impact
Likelihood
Minor
Moderate
Significant
Low Med
Medium
Med Hi
High
Likely
Low
Low Med
Medium
Med Hi
High
Possible
Low
Low Med
Med Hi
Med Hi
Low
Low Med
Low Med
Low
Low
Low Med
Medium

Why Risk Matrices Can Lead to Worse Decisions

- Illusion of communication
- Analysis placebo

Courtesy: Doug Hubbard and Behavioralize



What's the Alternative?

Quantification of Risk!

Probability of loss x magnitude

You don't have to become an actuary, but you can start thinking about risk like insurance companies do and ask for quantified risks

Common Objections Quantifying Risk

Objection 1: Quantifying risk is for insurance industry analysis and is unlikely to be appreciated by local governments looking for practical advice.

Answer: It is common for us to underestimate the capabilities of other people relative to our own. GFOA has presented quantified risk information to many elected officials and government staff and has yet to find one who could not at least grasp the essential point. As for practicality, given that subjective methods (like a risk matrix) often lead to worse decisions, we would suggest that it is the subjective methods that don't work in practice.

Objection 2: The cyber insurance market is volatile, so decisions based on a quantitative model will be wrong.

Answer: Insurance companies have been making decisions based on quantitative methods since the 17th century.

It is understood within the insurance industry that it would be foolish to attempt to compete without quantitative methods.

Objection 3: Within cybersecurity, there are too many complexities changing too quickly to make an accurate assessment.

Answer: One way or the other, a government has to decide on how to invest in commercial insurance, self-insurance, and controls for cybersecurity. A government can either take a wild guess and hope for the best or take a more rigorous approach.

Let’s See Some Data!

Ransomware Damages Follow a Skewed Distribution

Note: I focus on ransomware specifically, not cyber attacks generally

The <u>median</u> cost of a SME* ransomware attack in 2021: $98,000

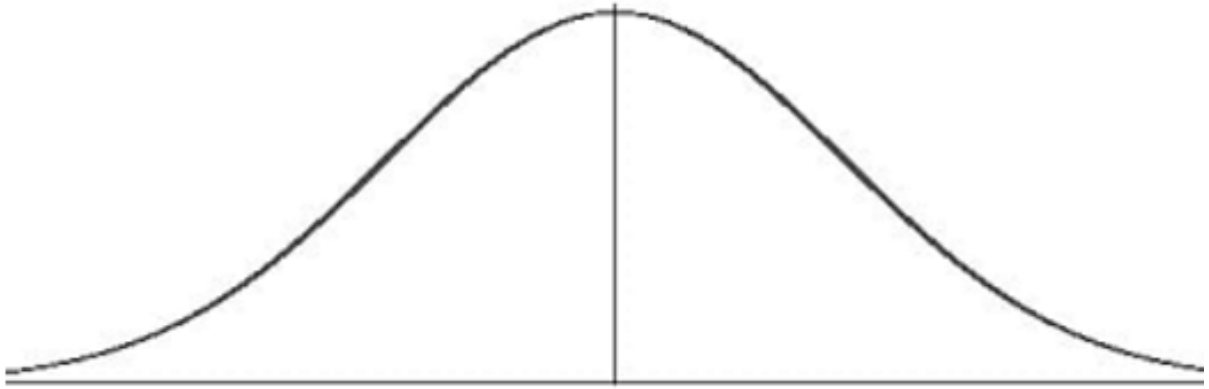
The <u>average</u> cost of a SME* ransomware attack in 2021: $267,000

The Jeff Bezos Problem

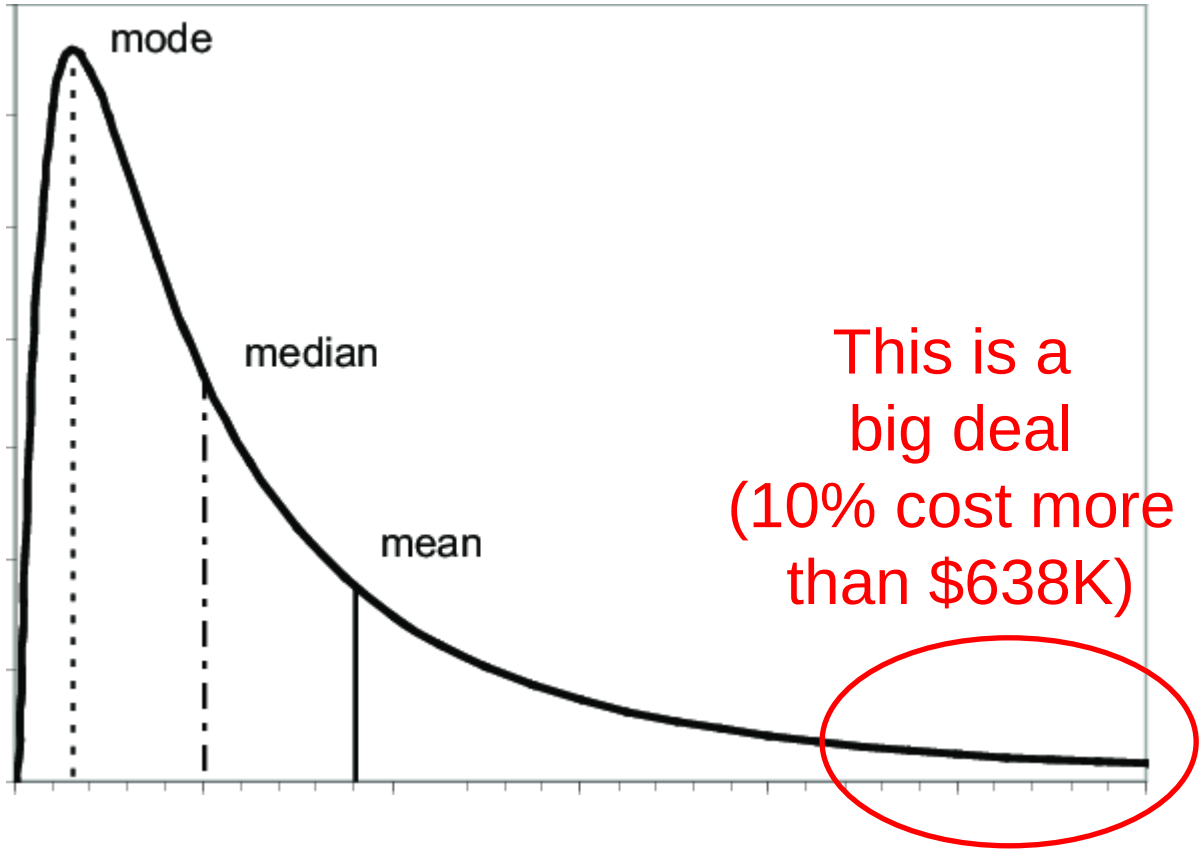
Small / Medium Enterprises defined as less than $2B annual revenue

Courtesy: NetDiligence

We are **not** dealing with this (mean, median, mode are in the middle)



We **are** dealing with this



This is a big deal (10% cost more than $638K)

Distribution of ransomware attack costs are more like natural catastrophes than snowfall, employee health care

Ransomware costs are not stable

Courtesy: NetDiligence

Ransom Demands and Costs Steadily Increasing

Ransom demands, forensics, and total incident costs have been calculated from the combined datasets.

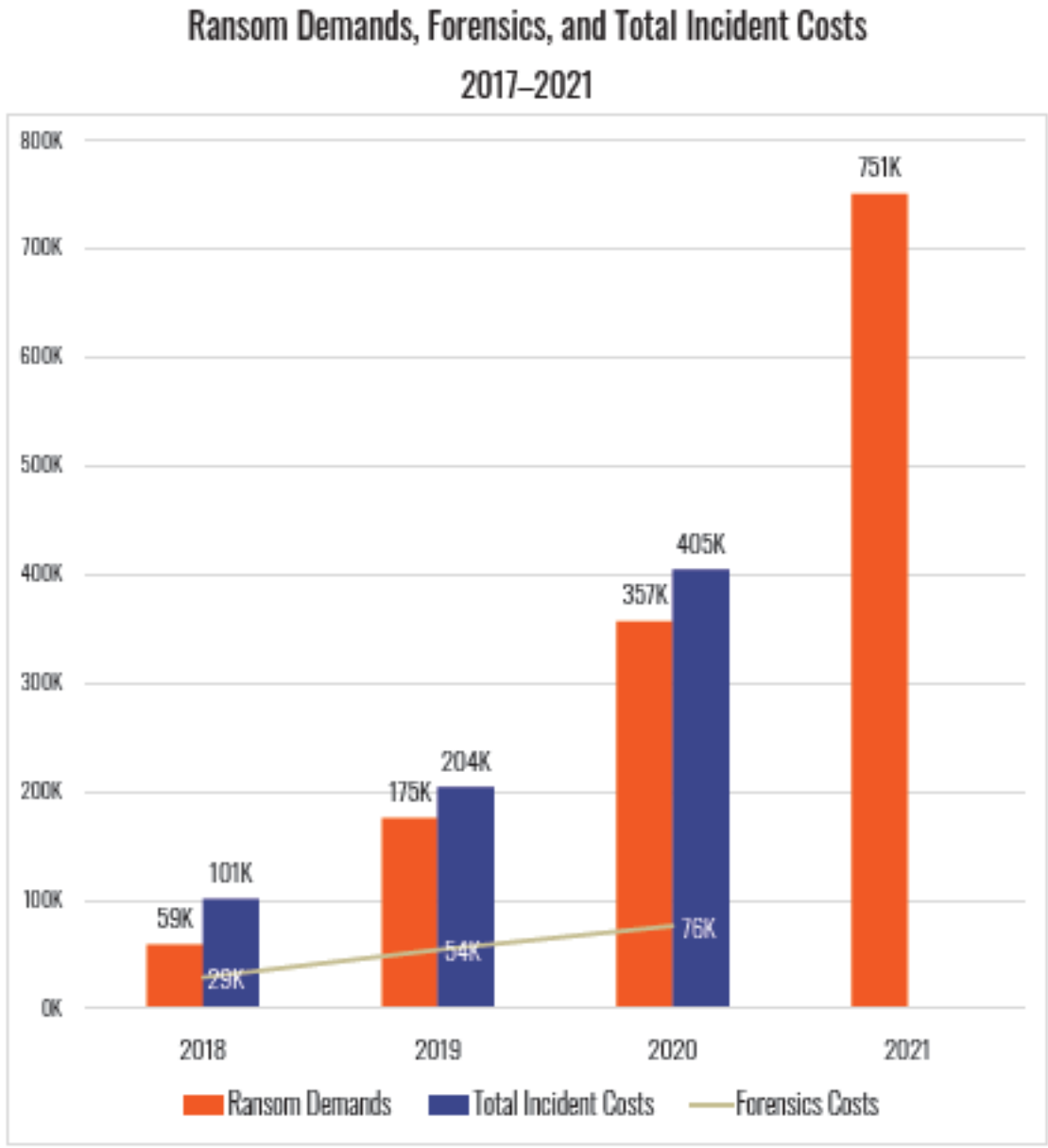


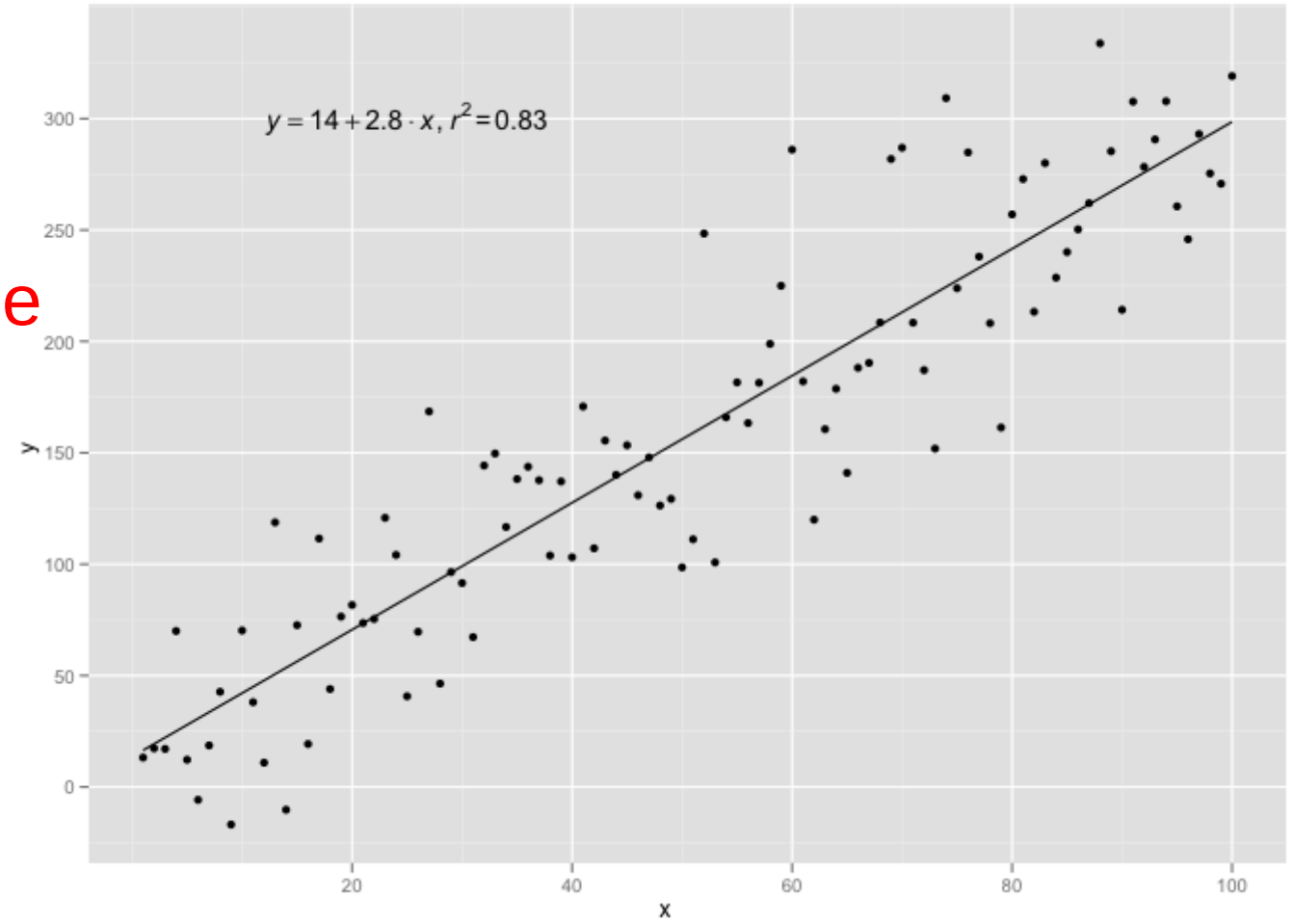
Figure 1

Damages are Only Weakly Related to Organization Size

This is an example of a scatter plot of a linear relationship.

The size of the government would predict the revenue loss from a recession with reasonable accuracy.

Revenue Loss from a Recession*



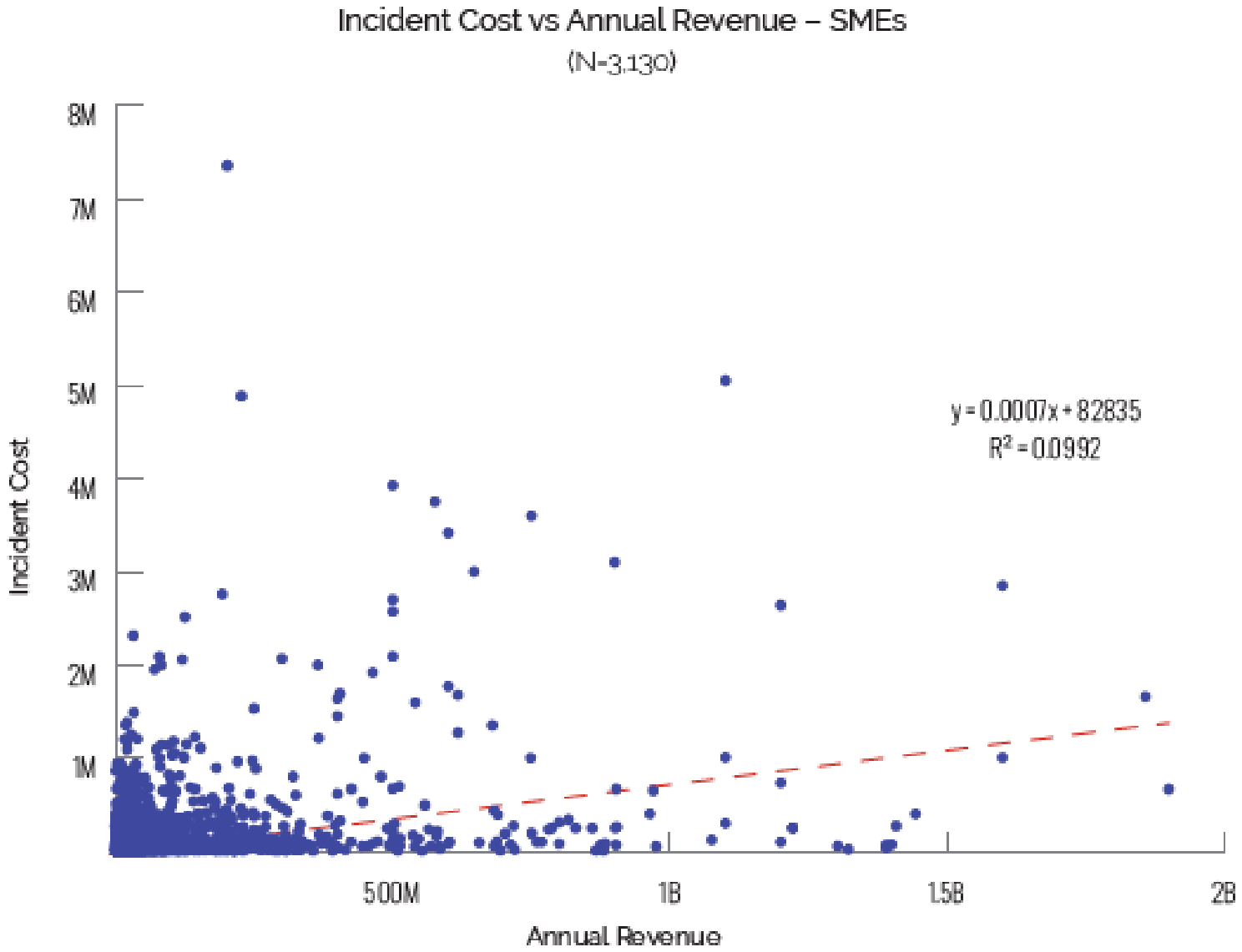
*Sample data for demonstration purposes only

Damages are Only Weakly Related to Organization Size

This is a scatter plot of ransomware incident costs compared to annual revenues for small and medium enterprises.

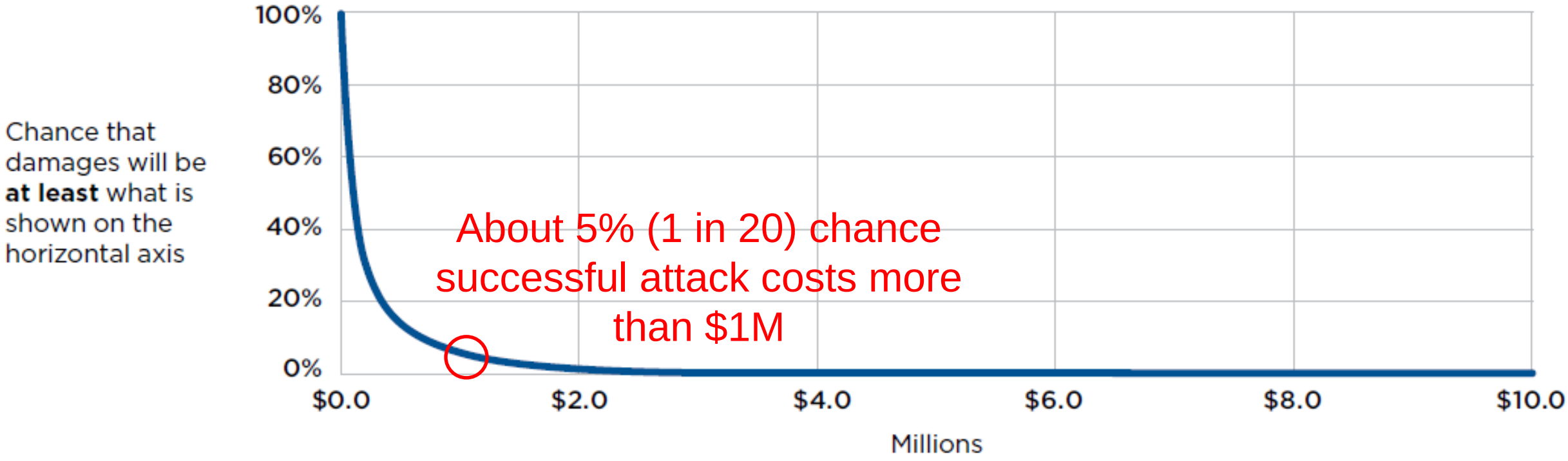
It looks very different!

Courtesy: NetDiligence

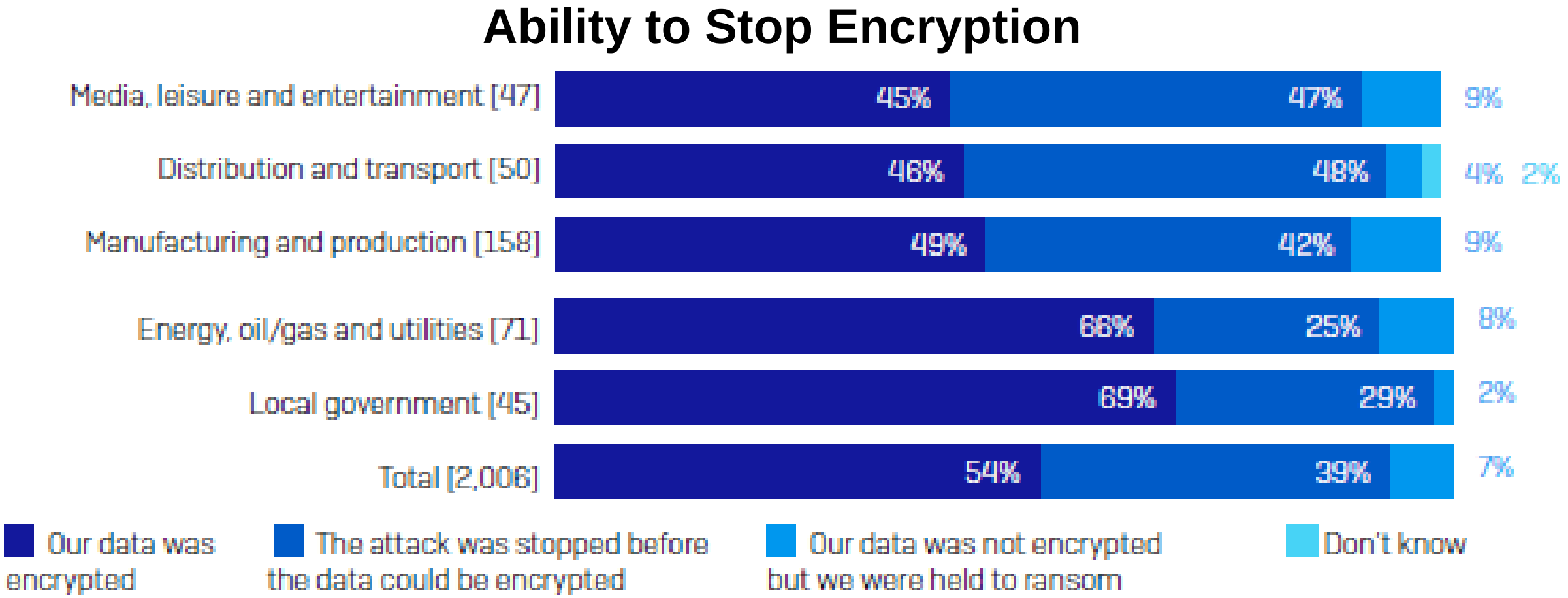


Loss Exceedance Curves

EXHIBIT 1 | LOSS EXCEEDANCE CURVE FOR A SUCCESSFUL RANSOMWARE ATTACK



Local Government Has a Lot of Opportunity for Investing in Better Cyber Security Controls

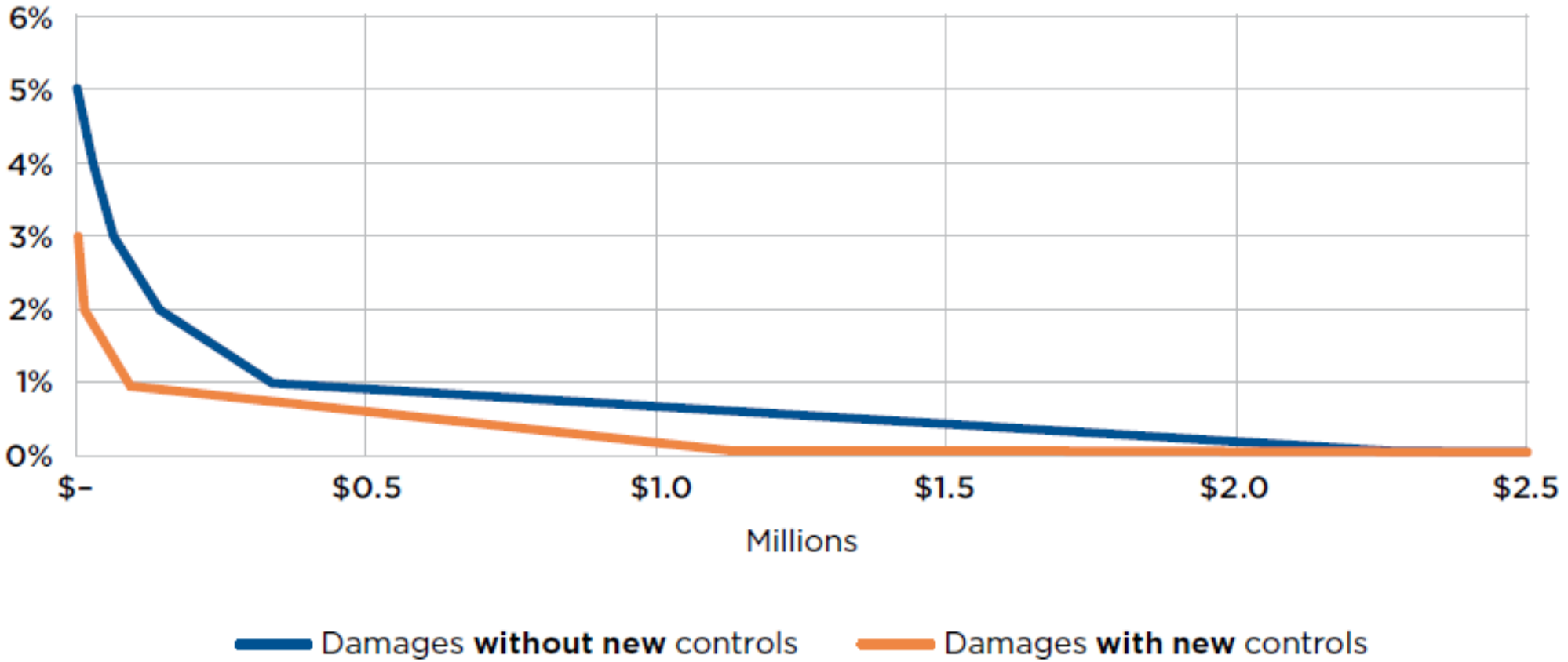


Source: Sophos

Investing in New Controls

EXHIBIT 3 | LOSS EXCEEDANCE CURVE WITH THE IMPACT OF NEW CONTROLS ADDED

Chance that damages will be **at least** what is shown on the horizontal axis

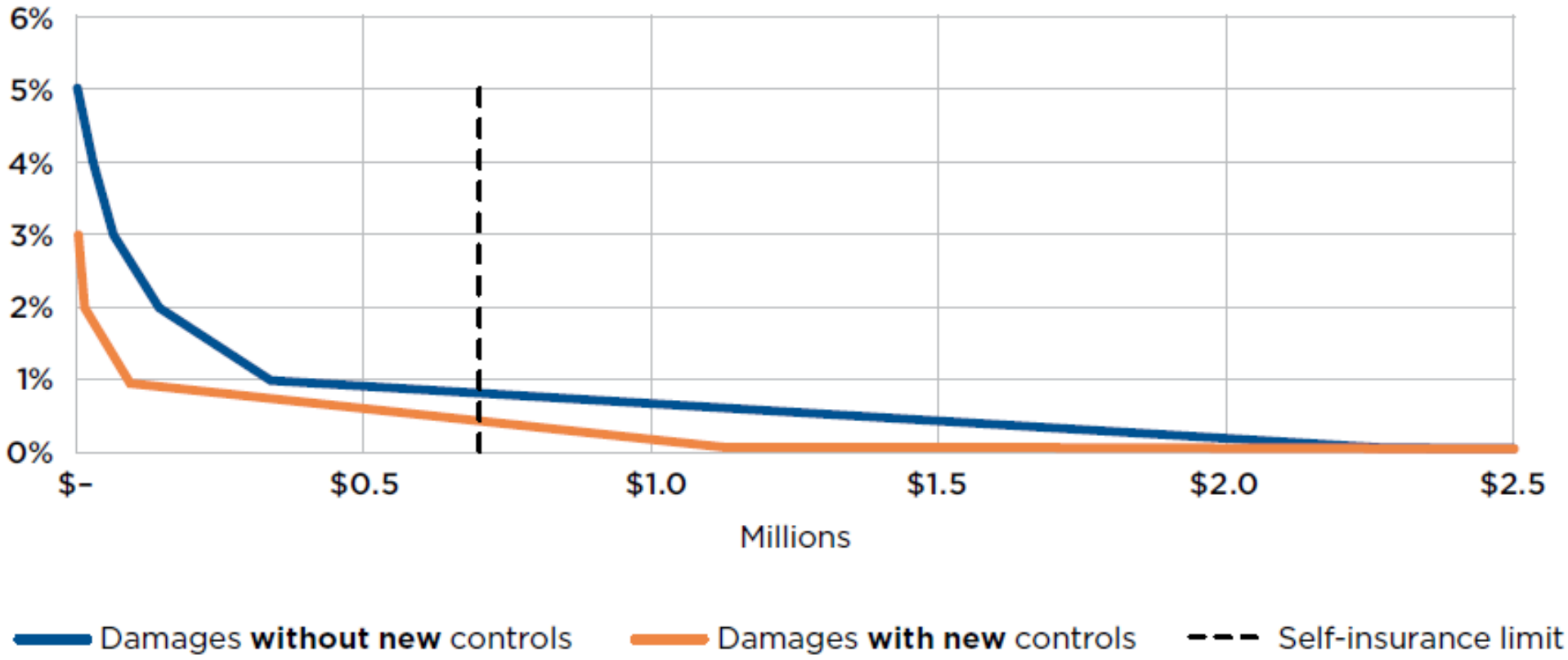


Let’s Talk Insurance

Don’t Overlook Self-Insurance

EXHIBIT 4 | LOSS EXCEEDANCE CURVE WITH AN AMOUNT AVAILABLE FOR SELF-INSURANCE

Chance that damages will be **at least** what is shown on the horizontal axis



Key Questions to Ask: How much do we have available for self-insurance? How does that compare to opportunities to invest in new controls or to buy commercial insurance?

Underwriting

- Underwriters are looking for key security features as a prerequisite for a policy.
- Such features might include: multi-factor authentication, incident response planning, encrypted data storage, patching cadence, and endpoint detection response.
- Governments with inadequate internal security might have trouble getting a policy or face increased costs.

Key Questions to Ask: How can you make the best impression on your underwriters to convince them you are a good risk? Do you have cost-effective opportunities to improve your security controls?

“The renewal quote has nearly doubled, and the retention amounts, particularly for ransomware incidents, have increased substantially…”

“Upon renewal, the insurance provider needed a brand new questionnaire with far more significant requirements…. As a result, we have been declined for this year and are working to see if we can get back onside with the requirement.”

Payout Limits and Sublimits

- Sublimits are a limit on the reimbursable loss for particular type of risk that is less than the total limit on the entire policy.
- The savvy customer will review all policy language and make note of any sublimits.
- Sometimes, sublimits are clear on the declarations page of the policy, but other times not! Common sublimits are:
  - Ransomware
  - System failure
  - Bricking

Key Questions to Ask: What are the sublimits in your policy? Do these sublimits change your understanding of the level of coverage you have? What implications does that have for your investment in cyber insurance (commercial or self-insurance) versus cyber controls?

Retentions

- High versus low retention – which is best?
- Your exposure beyond your policy limit is also “retention”
- Single highest retention vs multiple retentions

Key Questions to Ask: What balance between retention (self-insurance) and policy price (commercial insurance) is best for you? Is your policy single highest retention?

EXHIBIT 6 | SINGLE RETENTION VS. MULTIPLE RETENTIONS

	Retention
Security liability	$500,000
Regulatory liability	$500,000
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000

Attack happens and triggers these policies:
PCI (payment card industry)
Breach response
Business interruption

If you had **Single Highest Retention**:	
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000
You pay **max** of the group above	**$750,000**

If you had **Multiple Retentions**:	
PCI (payment card industry)	$500,000
Breach response	$750,000
Business interruption	$500,000
You pay **sum** of the group above	**$1,750,000**

Panel Requirements

- Know any requirements that you secure assistance from pre-approved cyber security contractor in the event of a breach
- If you use a cybersecurity contractor that is not on the insurer's list of approved providers then you may lose all coverage for breach response

Key Questions to Ask: What obligations do you have to use a specified security contractor to help respond to a breach? What options do you have to select between contractors?

Exclusions

- Exclusions are policy provisions that waive coverage for certain risks or loss events.
- An evolving issue is federal (and state) government policy on responding to ransomware attacks.
- Another sticky area is exclusions of “acts of war”.
- An exclusion with broader implications than just ransomware is if the insurance policy lists specific types of hardware, data, or other IT assets that are excluded from the policy.

Key questions to ask: What exclusions does the policy contain? What are the exclusions specific to ransomware attacks? What are the exclusions for particular types of IT assets you might own?

Definitions

- Be aware of provisions on when the insurance provider must be notified of claims and how that relates to your knowledge of when an insurable event has happened
- Be aware of definitions around internal security control standards you are required to maintain as a condition of the policy

Key questions to ask: Do you understand important definitions in your policy, such as requirements to use specified cyber security contractors when responding to a breach, notice of claims, and security standards?

Last Pitfall

- A pitfall is buying a policy that is overly focused on a narrowly defined risk
- Insurance customers can fall into this trap due to “recency bias”.
- Make sure that past first-hand experiences with cyberattacks or stories from peer governments aren’t being over-weighted in the design and selection of insurance policies to protect against future and evolving risks.

Key questions to ask: Are past (and painful) experiences with cyberattacks clouding your judgment in preparing for future risks? Is your cyber insurance policy too narrow and not providing adequate coverage for evolving threats? If a broader policy is cost-prohibitive might you be better off investing in preventative cybersecurity?

Getting Prices and Offers

- **Claims payment history:** Do customers actually get the coverage they thought they were buying? As we saw, limitations can cause customer to recover less than they thought they bargained for.
- **Pre-breach offerings:** Can the insurer offer useful advice for strengthening your preventative posture?
- **Flexibility on vendor utilization:** Does the insurer offer a reasonable number of options on contractors to support you in the event of a breach?
- **Experience in public sector:** Does the insurer understand the risks that characterize the public sector?

Remember: Insurance is most useful for extreme conditions

Ask: Can We Pool Risk?

Check out the report for more details and links to other resources like those shown in this presentation