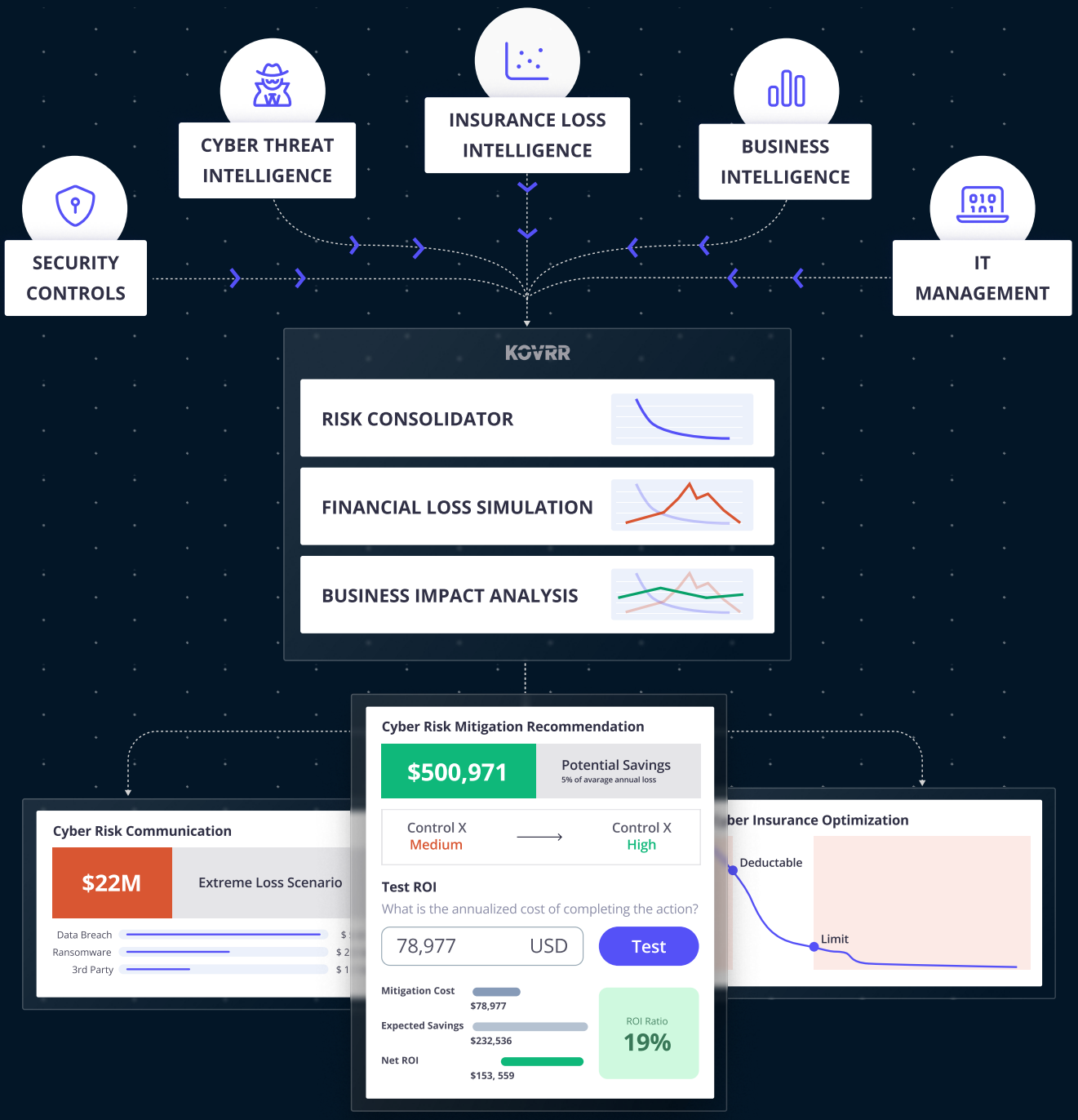
KOVRR



Material Cyber Event Analysis

eMerchify **November 29, 2023** *Q4*

What is a Material Cyber Event?

The Securities and Exchange Commission (SEC) has introduced regulations that mandate companies to report cyber events that result in a material impact.

However, what constitutes "material" varies significantly and is a complex legal issue. Materiality can be defined by several factors, including the duration of the event, the number of records compromised, and the extent of financial loss incurred.

Essentially, materiality is a contextual concept, and its determination requires a case-by-case evaluation. For some organizations, a breach might be considered material if it lasts for an extended period, while for others, it could be the compromise of a substantial number of records or a significant financial loss that deems a cyber event as material.

In navigating these SEC regulations, companies must carefully assess the unique circumstances and potential implications of cyber events to ensure compliance and transparency.

Kovrr recognizes the challenges in defining these thresholds. We offer assistance in setting preliminary values based on industry standards and best practices.

We also provide tools and expertise to help you investigate and analyze the likelihood of experiencing such material events and strategies to minimize this likelihood.

Note that you have the flexibility to edit and customize these thresholds as needed to align with your organization's specific risk profile and regulatory requirements.

Materiality Thresholds

Preliminary Material Financial Loss

The default threshold for defining material loss is set at $44.9M. This value is determined as a percentage of your company's annual revenue, which is $4.49B, equating to 1%.

1% of Revenue (100 BPS)

Other suggested thresholds

0.01%	$**449**K	1 BPS
0.1%	$**4.49**M	10 BPS
1%	$**44.9**M	100 BPS
5%	$**224**M	500 BPS
10%	$**449**M	1,000 BPS

Preliminary Material Amount of Records Compromised

The default material amount threshold is 11,000 data records. This value is set as a proportion of the 110,000 data records stored together in your company, accounting for 10%.

10% of Max stored together (110K)

Other suggested thresholds

1%	**1,100**
5%	**5,500**
10%	**11,000**
15%	**16,500**
20%	**22,000**

Preliminary Material System Outage Duration

The default threshold for the material event duration is set at 24 hours. This value is determined based on your response to the relevant question within the company sphere.

24
Hours

Normalized Average
Across All Asset Groups

Other suggested thresholds

24 h	100%
30 h	125%
36 h	150%
42 h	175%
48 h	200%

Likelihood Analysis

01 Preliminary Material Financial Loss

You have

41.45%

chance to have an event that exceeds the 0.01% of revenue **(449K USD)** threshold next year.

You have

26.66%

chance to have an event that exceeds the 0.1% of revenue **(4.49M USD)** threshold next year.

You have

6.25%

chance to have an event that exceeds the 1% of revenue **(44.9M USD)** threshold next year.

You have

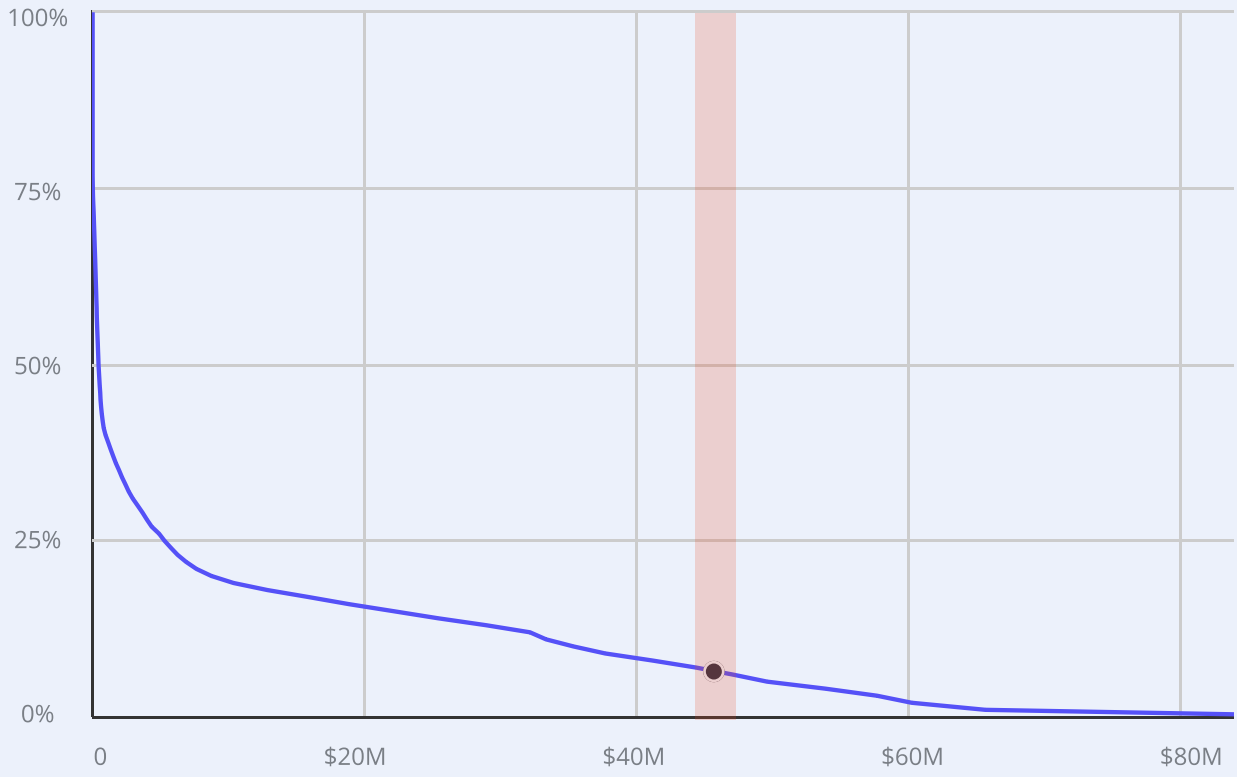
~0%

chance to have an event that exceeds the 5% of revenue **(224M USD)** threshold next year.

%

The single event maximum cost per year

By Likelihood



LET'S TAKE A CLOSER LOOK

Events that exceed the 1% of revenue financial threshold:

63%

of them are **Data Breach** Events

Their Median Loss:

$51.4M

24%

of them are **Ransomware** Events

Their Median Loss:

$70.17M

13%

of them are **Interruption** Events

Their Median Loss:

$47.73M

82.5%

of the Ransomware events result with impacts: **Availability and Extortion**

Their Median Loss:

$76.05M

17.5%

of the Ransomware events result with impacts: **Availability, Confidentiality and Extortion**

Their Median Loss:

$51.43M

Median Duration

5 days

Full Range: **1-30 days**

Median Number of Records Compromised

35K (32%)

Full Range: **6.1K (4%) - 109K (99%)**

Likelihood Analysis

02 Preliminary Material Amount of Records Compromised

You have
8.59%
chance to have an event that exceeds the 1% of records compromised **(1.1K)** threshold next year.

You have
8.59%
chance to have an event that exceeds the 5% of records compromised **(5K)** threshold next year.

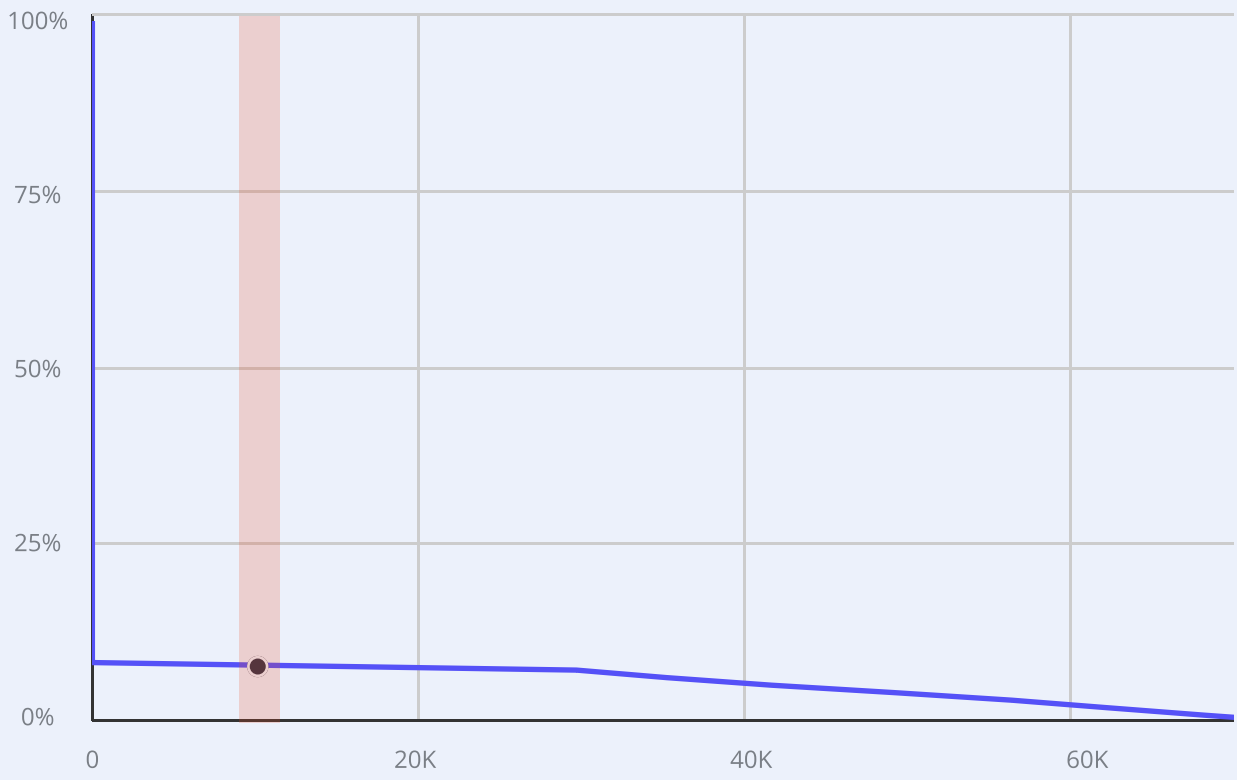
You have
8.33%
chance to have an event that exceeds the 10% of records compromised **(11K)** threshold next year.

You have
8.23%
chance to have an event that exceeds the 15% of records compromised **(16.5K)** threshold next year.

You have
8.16%
chance to have an event that exceed the 20% of records compromised **(22K)** threshold next year.

%

The single event maximum records compromised per year
By Likelihood



LET'S TAKE A CLOSER LOOK

Events that exceed the 10% of data records threshold:

70.2%

of them are **Data Breach** Events

Their Median Loss:

$890K

29.8%

of them are **Ransomware** Events

Their Median Loss:

$5.71M

74%

of the Data Breach events result with impact **Confidentiality**

Their Median Loss:

$606K

26%

of the Data Breach events result with impacts: **Availability and Confidentiality**

Their Median Loss:

$2.1M

Median Duration

3 days

Full Range: **1 hour - 30 days**

Median Number of Records Compromised

12K (11%)

Full Range: **11K (10%) - 109K (99%)**

Median Cost Per Record

$10.45

Average: **$11.13**

Likelihood Analysis

03 Preliminary Material System Outage Duration

You have
31.25%
chance to have an event that exceeds the **24 hours** threshold next year.

You have
27.34%
chance to have an event that exceeds the **30 hours** threshold next year.

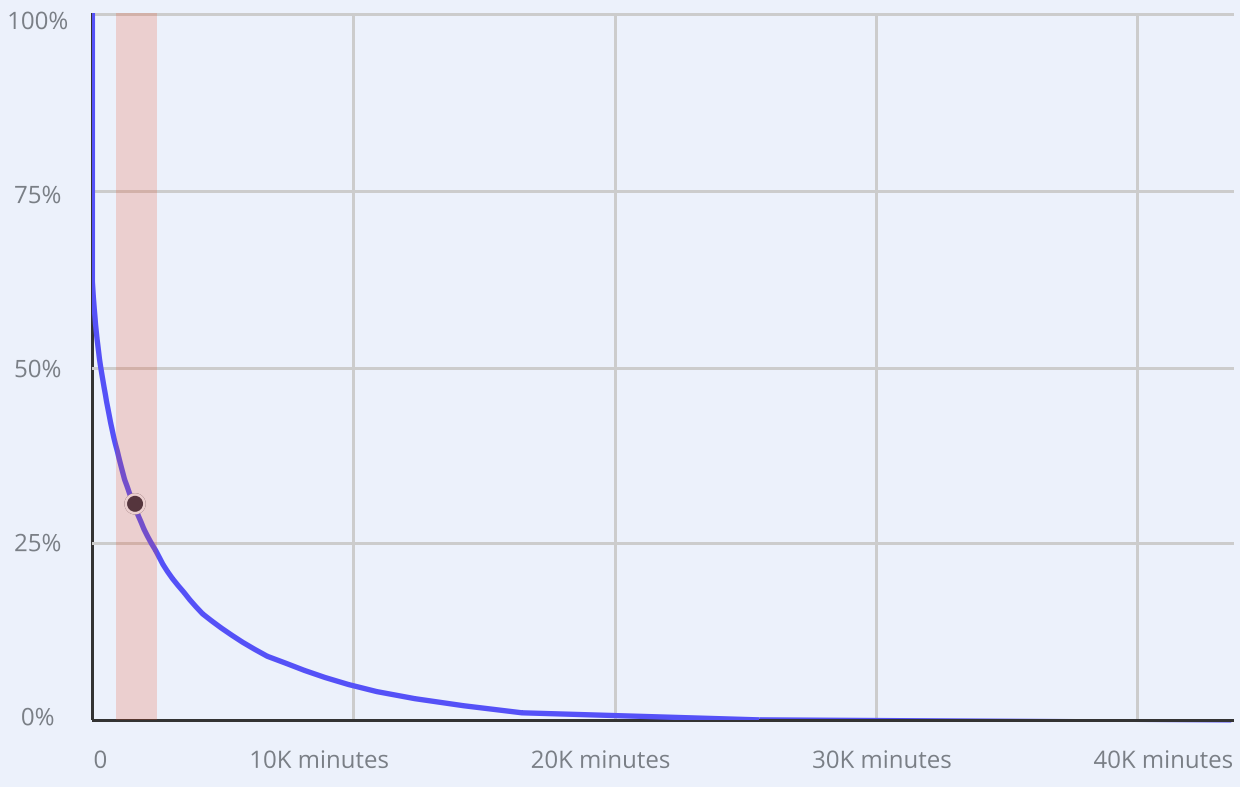
You have
25.13%
chance to have an event that exceeds the **36 hours** threshold next year.

You have
22.22%
chance to have an event that exceeds the **42 hours** threshold next year.

You have
19.44%
chance to have an event that exceeds the **48 hours** threshold next year.

%

The single event maximum outage duration per year
By Likelihood



LET'S TAKE A CLOSER LOOK

Events that exceed the 24 hours event duration threshold

43.3%

of them are **Interruption** Events

Their Median Loss: $423K

37%

of them are **Data Breach** Events

Their Median Loss: $4.52M

19.7%

of them are **Ransomware** Events

Their Median Loss: $6.69M

34.3%

of them result with impact **Availability**

Their Median Loss: $423K

30.1%

of them result with impacts: **Availability and Extortion**

Their Median Loss: $5.89M

26.4%

of them result with impacts: **Availability, Confidentiality and Extortion**

Their Median Loss: $6.95M

9.2%

of them result with impacts: **Availability and Confidentiality**

Their Median Loss: $4.52M

Median Duration

34 hours

Full Range: **24 hours - 30 days**

Median Number of Records Compromised

21K (19%)

Full Range: **0 - 109K (99%)**

Average Cost Per Hour of Operation

$700K

Average: **$220K**

Kovrr's Cyber Materiality Report allows you to

- Determine which cyber risks are likely to meet materiality thresholds, rendering them suitable and applicable for annual report disclosures (10-K, 20-F)
- Create a data-driven framework for quickly aligning incidents to risk to know if a material disclosure is advisable within the given 4-day period (8-K)
- Confidently communicate the state of the organization's cyber posture and what the cyber program recommends qualifies as preliminarily material to legal counsel and the board of directors