FACT SHEET

Interactive Cost Model (ICM)

SAFE

Empower your board with a defensible *and trustable* dollar-value estimate of your financial risk due to cyber attack

Security, IT, and board executives are all under increasing pressure and scrutiny to **prove that their security programs adequately manage their risk exposure**, and to provide a response to a crucial question:

"How much would a cyber attack cost our organization - and how can we reduce it?"

Organizations find they **either lack this dollar value, or fail to understand its logic**. Commonly available, 'blackboxed' simulators produce results that impede effective risk management - reducing strategic conversations to decisions based on guesswork. Security leaders are unable to confidently answer:

"How can we maximise our business risk reduction with our current security budget?"

If they're to keep pace with an evolving threat landscape and secure the confidence of major stakeholders, **today's leaders require tools that blend internal diagnostics with threat intelligence** to produce a bespoke, accurate, financial analysis of cyber risk.

Delivering Value Across Your Organization

For CEOs, Board Members

- Gain an **objective, automated, and real-time** view of $ value business risk. No manual SME inputs required. Measure ROI of cybersecurity initiatives to prioritize investments.

For CISOs, CFOs

- **Explainable, accurate, and trusted** $ risk values per attack type. **Dynamically connect security controls to $ risk** for data-driven board conversations and insurance renewals.

For Risk and Insurance Practitioners

- Fully **customizable, driver-based model** with benchmarks backed by extensive research. Get inside-out risk assessment combined with outside-in.

The first interactive cost model calculating dollar-value risk per attack vector

Replace heatmaps and scores with dollars and cents
Understand the estimated financial impact of cyber risk in a business context - bespoke to your organization.

Gain trusted, defensible estimates you can justify
Manage your inherent cyber risk by tuning cost drivers to reflect your internal modeling assumptions.

Understand risk drivers and customize your results
Use the default drivers or tune them to get your Annual Loss Expectancy* and Estimated Financial Impact**.

Driven by data, powered by research
Leverage proprietary cyber attack cost data sourced from over 5400 discrete attack costs, plus more.

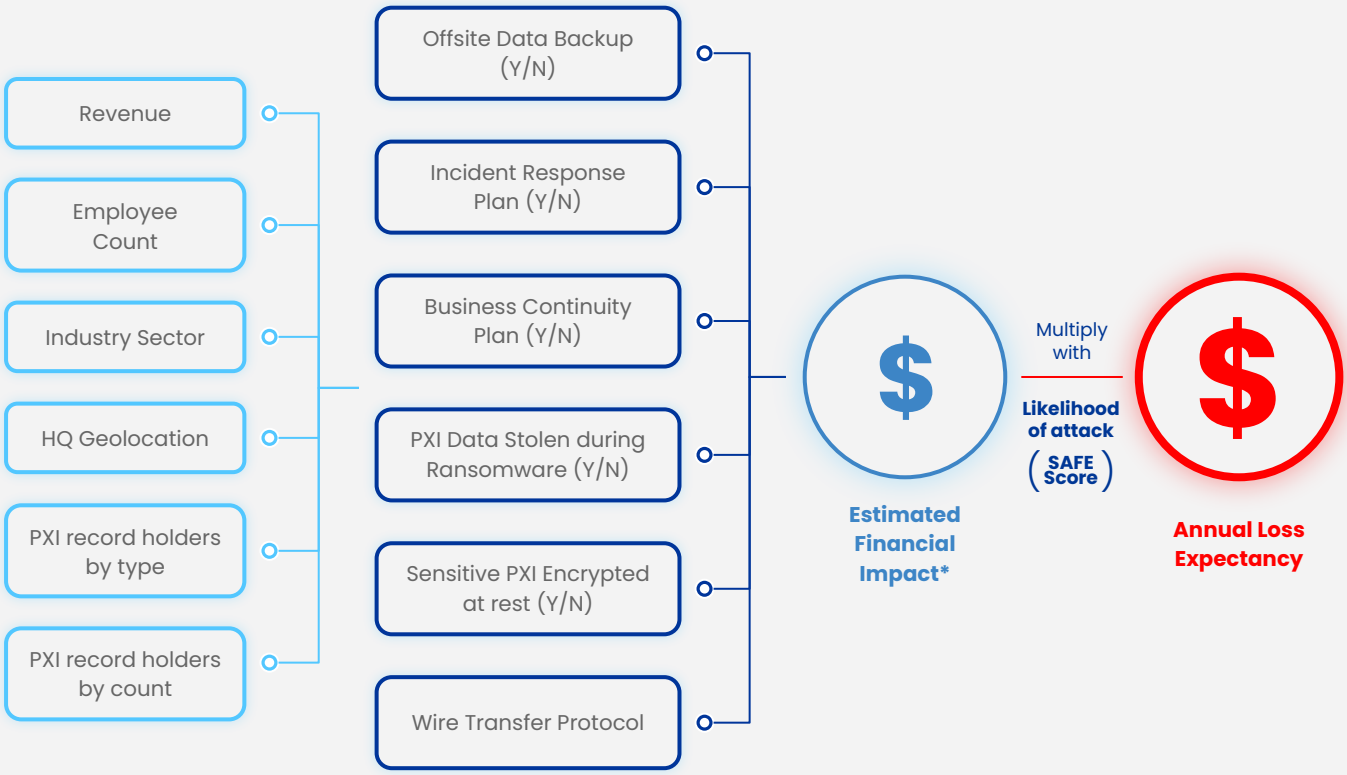
Enabling True Cyber Risk Quantification and Management

Only SAFE, with its inside-out SAFE scoring model and bottom-up, tunable ICM,
links financial residual risk with your digital assets via the controls protecting them

*__Annual Loss Expectancy__: The product of the estimated financial impact from cyber risk times the annual likelihood of that risk occurring.
** __Estimated Financial Impact:__ The $ cost of one or more cyber attacks (were those attacks to happen); expressed by upper bound, expected, (mean), and lower bound values.

How the Interactive Cost Model works

The ICM automatically calculates the Estimated Financial Impact based on 12 inputs. At each cost category level there are cost drivers that can be tuned by the customer, or they can use the default drivers generated by the initial EFI.



* Hyper detailed for ransomware, data breaches and business email compromise

Why ICM outperforms existing commercially-available models

Commercially available models	Safe Security Interactive Cost Model
Subjective and assumption-driven input data	API-driven input ensuring quality control of data
Aggregated, top-down modeling	Driver-based modeling leveraging business data
Confidence yield: Low; due to opaque design and methods	Confidence yield: High; due to transparent, customizable model design
Dollar-value outputs require manual SME-based inputs using outside-in analyses	Objective, automated, real-time view via inside-out and outside-in data, bespoke to your organization
Blackbox approach; single dimension assessment	Defensible, evidence-backed dollar-values for total enterprise view, as well as per attack type
Simplistic model; research depth: low-medium	Comprehensive model; extensive expert-led research and benchmarking

Research

Safe Security's dedicated research analysts have examined thousands of security incidents, extracting attack related costs from open source information, and by performing financial analysis on key filings. **This provides us with the understanding of the costs associated across different security incidents**, and if a certain type of attack or pre-attack security posture is likely to lead to regulatory investigations or litigation.

Model Design

The Interactive Cost Model **is capable of conforming to different internal assumptions for cost modeling.** It uses granular attack costs to model the upper and lower bounds, plus the mean, wherever possible for default cost drivers (see figure below). **It goes beyond surface-level, aggregated settlement-paid totals by using drivers that comprise the different elements of a settlement.** For example, litigation cost drivers includes drivers that generate claims, attorneys' fees, monitoring, and ID protection costs. Likewise, Business Interruption includes the categories of revenue lost or deferred, net profits lost, contract penalties, and resourcing expenses accrued.

The ICM is powered by **Safe Security's proprietary database** - built and maintained by our expert analysts and threat intelligence teams. The model leverages:

- Over **500,000 data points** across **2,000 mapped discrete incidents** taken from primary sources across:
  - Financial fraud - such as business email compromise, account takeover, and advertising fraud
  - Ransomware, PxI data breaches - including leaks and exposures
  - Wiper and cryptocurrency theft - including lost access
  - Data privacy violations
- **~1300 CVEs** identified as seen in the wild., and **over 1,100 attack groups** including identified aliases
- **TTP mapping to MITRE ATT&CK** for over 100 attack groups and malware (with more added regularly)
- A pipeline of over 25,000 security incidents being actively reconciled and processed.

To provide the granularity necessary for default cost driver modeling, all discrete attack costs are mapped by:
:

- Incident mapped to timeline and attribution
- Entity attacked geolocation and revenues
- Parent attack type, sub attack type
- Campaign type and data source
- Direct or indirect cost
- PXI contents such as PHI, PII, PFI, and PCI
- Pre-attack cybersecurity posture
- Consent order details, if applicable, **and much more**

	Upper Bound	Expected	Lower Bound
TOTAL RANSOMWARE + DATA BREACH + BEC	363.0 M	60.4 M	3.6 M
TOTAL RANSOMWARE	137.3 M	29.8 M	2.4 M
TOTAL DATA BREACH	225.6 M	30.5 M	1.2 M
TOTAL BEC	0.0 M	0.0 M	0.0 M
RANSOMWARE ATTACK	**137.3 M**	**29.8 M**	**2.4 M**
Incident Response (IR)	4.6 M	2.7 M	0.8 M
Business Interruption (BI)	76.7 M	18.4 M	0.2 M
Restoration (RE)	19.4 M	4.9 M	0.7 M
Customer-Employee Support (CES)	1.2 M	0.0 M	0.0 M
Regulatory & Litigation Defense (RLD)	6.3 M	3.2 M	0.6 M
Litigation (L)	29.1 M	0.7 M	0.0 M
DATA BREACH ATTACK	**225.6 M**	**30.5 M**	**1.2 M**
Incident Response (IR)	2.6 M	1.3 M	0.3 M
Customer-Employee Support (CES)	2.4 M	0.4 M	0.0 M
Regulatory & Litigation Defense (RLD)	6.3 M	3.2 M	0.6 M
Litigation (L)	190.0 M	25.0 M	0.3 M
Regulation (RG)	24.3 M	0.7 M	0.0 M
BEC ATTACK	**0.04 M**	**0.04 M**	**0.03 M**
Cash Stolen (CS)	0.03 M	0.03 M	0.03 M
Incident Response (IR)	0.01 M	0.01 M	0.00 M

For more information, visit https://safe.security/interactive-cost-model