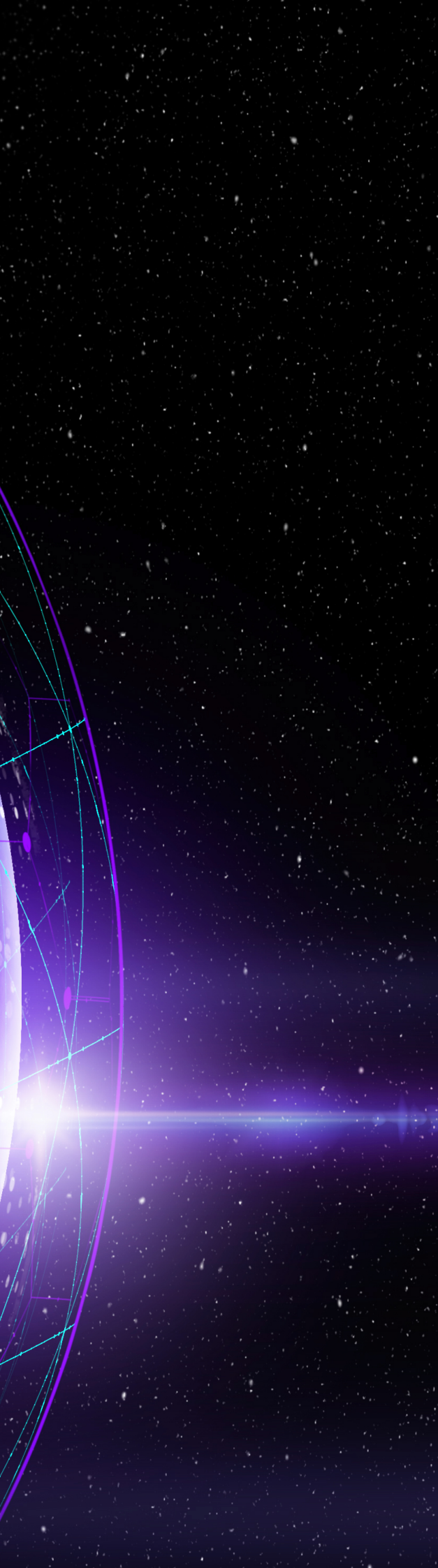


# The Day After: Toting Up the Costs of a Catastrophic Cyber Attack

---

MARCH 2022



What will a catastrophic cyber attack cost your business? The go-to answer to this important question is \$4.24 million, according to the respected annual Ponemon Institute “Cost of a Data Breach Report.” That’s the average cost of a breach, based on their research. With all due respect to the Ponemon Institute, however, that figure is not actually very helpful.

For one thing, it’s an average. The average price of a new car might be \$47,000 in the US right now (ouch!), but the car you’re driving might be an old junker worth \$500 or a Bugatti Chiron, which is yours for just \$3 million. Averages don’t always reflect your reality.

So, what does an extreme cyber attack really cost? When you sit down the day after the incident and tote up your costs, what are you looking at? This is a matter of [cyber risk quantification](#) (CRQ) for your unique business and the circumstances of the attack.

## It’s about Residual Risk

Managing cyber security is about risk management and risk modelling. In particular, the financial quantification of cyber attack damage is a matter of determining residual risk. That’s the risk your business faces after countermeasures and insurance have been taken into consideration. The good news here is that a serious cyber attack may have a real cost of zero dollars when seen from the perspective of residual risk. Of course, you may not be that fortunate.

## Understand the Financial Impact of Cyber Events on Your Business

Your business will have its own unique factors that determine the true financial impact of a serious cyber attack. That said, the experiences of your industry peers can be useful in estimating how a cyber attack might affect your business. Similar companies tend to experience similar losses. Kovrr’s CRQ software factors peer company loss data into its financial quantification process.

For example, if your business has a long customer list, then breach notifications will be more expensive than would be the case if you had relatively few customers. The cost to replace operational assets can vary greatly, as well. A cyber attack that paralyzes an office, for example, will result in fairly low costs. If you own an industrial plant, a destructive cyber-physical attack could cost tens of millions of dollars to remediate.



Kovrr assigns the costs of a cyber attack into three basic categories:

- + **Technology costs:** for repairing systems, restoring data, implementing new security countermeasures and so forth.
- + **Hard business costs:** covering the expenses related to legal and public relations, overtime, notification mailing campaigns and beyond.
- + **Soft business costs:** relating to reputational damage (which may require advertising to remediate) and impacts on employee morale and customer sentiment.

When you add these up, and compare them with the experiences of peer companies, you start to get closer to an accurate CRQ for your distinct business situation.

## Assess the ROI of Cyber Investments

Whatever your number is, it will help you figure out the value of investing in cybersecurity capabilities, services and solutions. Cyber security is a line item in your budget. Chances are, security managers have ideas for new spending coming up in the future. What, and how much should you approve, if any?

CRQ gives you the ability to assess your return on investment (ROI) for cybersecurity. For example, if your CISO wants to engage with a managed security service provider (MSSP) that will cost \$1 million a year, the question is whether the risks the MSSP can mitigate are worth more than a million dollars. You won't get an answer down to the penny, but if you've done accurate CRQ, you'll have a good idea about whether spending a million dollars on an MSSP will generate ROI.

It's possible the ROI will be based on a range of loss estimates. The CRQ process may determine that potential costs of a serious cyber attack are between \$800,000 and \$1,200,000. In that context, a million-dollar outlay for an MSSP is probably a wise investment. If the range is from \$10,000 to \$40,000, then the MSSP is not a good choice—at least at the scale it is being proposed.

## Prioritize Cyber Risk Management Decisions

Knowing the cost of a catastrophic cyber attack can also guide your priority of security investments. The best practice is to invest in protecting the most highly valued digital assets. CRQ can help you identify what those are, and what cost of defence will be justified. For instance, if email vulnerabilities are the biggest driver of cost for an attack, an investment in email security should take the highest priority over alternatives.

Kovrr financially quantifies cyber risk on demand. Our technology enables decision makers to seamlessly drive actionable cyber risk management decisions.

[Contact us to book a demo.](#)

## The Author



Tom Boltman

VP Strategic Initiatives

---

## About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: [contact@kovrr.com](mailto:contact@kovrr.com)