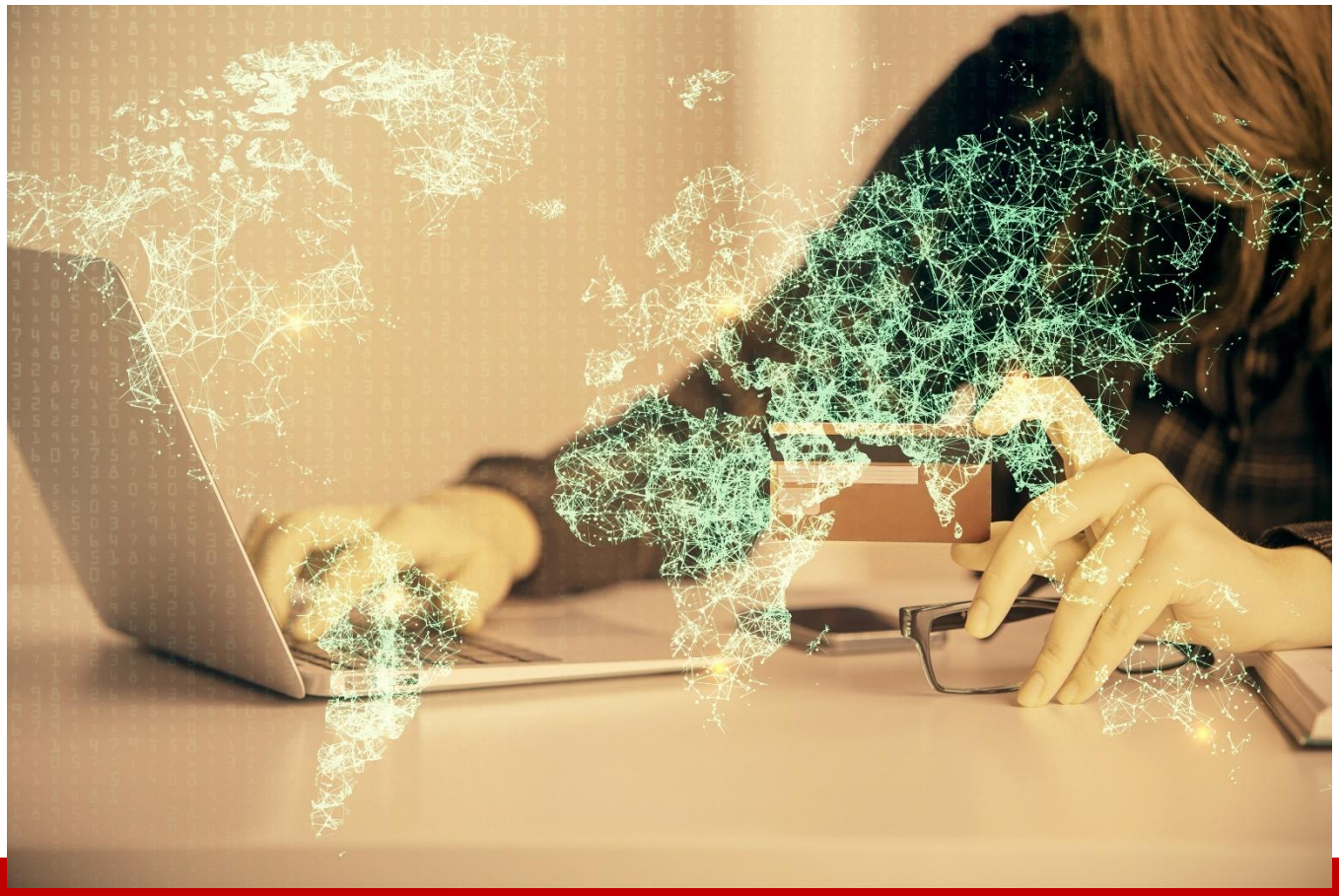

Impact Modeling Will Become a "North Star" of Cyber Resilience Planning in 2025

By Scott Kannry, Co-Founder and CEO, Axio

Traditionally, IT teams have relied on probability analysis as a primary guide for their resilience strategies. This meant assessing the likelihood that a specific type of cyber incident would occur and allocating resources to fortify high-risk systems and vectors, as needed. It's a useful framework that has—and will continue to—help companies surface potential threats and design strategies to address them. However, as the cyber landscape evolves, security teams must shift their approach as well.

In 2025, cyber incident impact modeling will take center stage as a primary driver of resilience planning. The growing consensus among security leaders is that overemphasizing probability can hinder rather than enhance resilience. By broadening their focus to include the consequences of incidents that *do* occur rather than solely emphasizing the probability of those that *might,* organizations will be better positioned to prioritize mitigation and recovery efforts.

The problem with an overreliance on probability analysis

An overreliance on probability analysis can create a false sense of security. For example, a threat deemed "low probability" may still carry devastating consequences if it materializes. A ransomware attack targeting operational technology (OT) systems, for example, while statistically uncommon, could paralyze critical infrastructure, halt production lines, or disrupt patient care.

This sole focus on probability can also lead to skewed resource allocations. An IT team, for example, might direct most of its efforts toward mitigating high-likelihood, low-impact incidents (e.g., phishing attempts) while neglecting preparation for low-likelihood, high-impact events. This misalignment can leave organizations vulnerable to the types of incidents that can cause the greatest harm.

Ultimately, probability analysis offers only part of the picture. By itself, it doesn't answer the question that decision-makers care about most: "What would happen if this threat became a reality?"

Why impact modeling matters

Impact modeling expands the conversation from "What are the chances of this happening?" to include, "What would happen if it did?" By focusing on tangible consequences—whether financial, operational, or reputational—security leaders can better understand and prepare for the cascading effects of a cyber incident.

This approach isn't just theoretical; it's driven by real-world events. Recent high-profile OT incidents have underscored the critical need to plan for impacts, not just probabilities. Here are a few recent examples from this year that should give any team pause:

- A mass tech outage in July forced **Delta Air Lines** to ground flights across multiple airports and caused significant delays for passengers. The financial fallout included lost ticket revenue, increased operational costs, and potential reputational damage from frustrated customers, highlighting how even a single event can cripple critical infrastructure.

- A month later, a ransomware attack targeting systems at **Seattle-Tacoma International Airport** led to widespread delays and logistical challenges. The incident demonstrated how dependent modern transportation hubs are on interconnected systems. A breach in one area can ripple through airport operations, affecting airlines, passengers, and downstream logistics partners.

- When the medical systems at **Lurie Children's Hospital** in Chicago were hit by a ransomware attack in January, it forced the cancellation of critical medical procedures. Beyond financial costs like lost revenue and incident response expenses, the attack raised life-or-death stakes, delaying urgent care for vulnerable patients and eroding public trust in the institution's ability to safeguard sensitive data and ensure continuity of care.

These examples illustrate how focusing solely on probability can leave organizations unprepared for the devastating consequences of these incidents. Impact modeling ensures that decision-makers prioritize the right resources to address these scenarios and develop robust recovery plans.

The rise of impact modeling in 2025

In 2025, impact modeling will no longer be a secondary consideration in resilience planning—it will take center stage. Security leaders are increasingly recognizing that understanding and preparing for the aftermath of an attack is just as important as preventing the attack itself.

For example, impact modeling enables organizations to:

- **Quantify financial exposure:** By estimating the potential costs of a cyber incident, from lost revenue to regulatory fines, organizations can better allocate budgets toward high-impact risks.
- **Prioritize critical systems:** Impact modeling helps identify which systems and processes are most essential to business continuity, ensuring they are adequately protected.
- **Enhance recovery strategies:** By simulating the downstream effects of a cyberattack, organizations can develop more effective response and recovery plans.

By adopting impact modeling, organizations will be better positioned to answer the “what if” questions that drive resilience. This approach provides actionable insights that help organizations proactively mitigate risks, reduce downtime, and minimize financial losses.

Balancing probability and impact

It’s important to note that impact modeling doesn’t replace probability analysis entirely; rather, it complements it. Probability analysis still plays a role in identifying likely threats and guiding preventive measures. However, by combining probability with impact modeling, organizations can achieve a more comprehensive understanding of their risk landscape.

This balanced approach ensures that security teams allocate resources wisely, focusing on both high-likelihood and high-impact scenarios. For example, a ransomware attack targeting sensitive customer data might have a low probability but catastrophic consequences. By integrating impact modeling into their planning, organizations can ensure they are prepared for even the most unlikely events.

Building long-term resilience

As cyber threats become more sophisticated and interconnected, resilience planning must evolve to keep pace. Impact modeling provides the clarity organizations need to navigate an increasingly complex threat

landscape. By focusing on tangible outcomes, security leaders can develop strategies that not only prevent incidents but also minimize their effects.

Understanding and preparing for the consequences of a potential attack has proven far more valuable to effective decision-making and long-term resilience. By placing impact modeling at the heart of resilience planning, organizations can ensure that their cybersecurity strategies align with business objectives, protect critical operations, and foster stakeholder confidence.

In 2025, impact modeling will no longer be a “nice-to-have”—it will be an essential tool for building and sustaining resilience. Security leaders who embrace this shift will be better equipped to protect their organizations from the ever-evolving cyber threat landscape.

About the Author

Scott Kannry is the Chief Executive Officer and Co-founder of Axio, a leading cyber risk management company. As the architect of Axio’s four-quadrant cyber loss impact taxonomy and methodology for evaluating and stress testing insurance portfolios, Scott spearheaded a novel process designed specifically to better align overall cyber exposure with insurability. This approach was the first to codify the reality that cyber predicated losses can trigger numerous lines of insurance coverage. Scott has been recognized as a 40 Under 40 broker by Business Insurance magazine, a power broker by Risk and Insurance magazine, and an industry rising star by Reactions magazine. Scott can be found on LinkedIn here.