



CASE STUDY

# How the Edge Solution Unified a Biotech's Cyber Incident Response

The biotech company was compelled to take action after a tabletop exercise engaged their executive team, revealing their vital role in company-wide incident response.

INDUSTRY

Biotech

REVENUE

\$500M-\$1B

FEATURES USED

BAS Tests

Tabletop Exercise

CONTEXT

This biotech company has over 5,000 employees and operates in more than 100 markets worldwide. One of their goals with their partnership with Resilience was to break down silos to ensure a high standard of preparedness during a cyber incident.

CHALLENGE

The organization faced difficulties in ensuring clear visibility across departments during incidents, particularly around roles and responsibilities. The IT and Security team felt that there was a lack of preparedness at the executive level.

SOLUTION

Through the Edge Solution, the IT/Security team tested their security preparedness with breach and attack simulation tests. These features helped the IT/Security team identify gaps in their security posture and upheld their hypothesis that the organization needed more support from the executive level.

In order to bring the executive team to the IT/Security team's level of understanding, the organization worked with Resilience experts to support a tabletop exercise (TTX), a simulated activity where their leadership and relevant teams could discuss and walk through how they would respond to a security incident. The goal of this tabletop exercise was to make the experience as uncomfortable as possible to stress-test the organization's readiness. While the exercise exposed the executive team's unpreparedness, it also showcased the IT team's competency and alignment.

This exercise sparked valuable discussions and brainstorming among the executives, ultimately helping them better understand their critical role in incident response and support changes in budget allocations.

RESULTS

- The TTX revealed a disconnect between executive and technical teams, significantly improving organizational awareness.
- The TTX brought potential areas of improvement in the company's incident response plan to light. This allowed the IT/Security team to make suggestions with clear support from management.
- Increased executive support led to new budget allocations for new and ongoing cybersecurity activities.



Discover the strategy that drove our success

CONTACT US

[ReachUs@cyberresilience.com](mailto:ReachUs@cyberresilience.com)

Please refer to your insurance quote for specific details governing your coverage. Insurance coverage presented herein is for informational purposes only. The terms and conditions of your specific insurance quote will govern. Certain conditions and limitations may apply. The purchase of insurance coverage is in no way tied to the purchase of security services. Nothing in these materials should be construed as an express or implied endorsement or recommendation of Resilience by any government or government agency. In the United States, insurance products are distributed by Ocrea Risk Services, LLC (NPN 19169260) d/b/a Resilience Cyber Insurance Solutions. Resilience products are underwritten by Homeland Insurance Company of New York or Homeland Insurance Company of Delaware, each subsidiaries of Intact Insurance Group USA LLC with their principal place of business at 605 Highway 169 N, Plymouth, Minnesota 55441. Arceo Labs, Inc. d/b/a Resilience provides security services through its expert security team.