Reevaluate Traditional Cybersecurity Training To Increase Your Team's Resilience

FORRESTER®

FIRMS FACE IMMENSE PRESSURE TO PREPARE FOR CYBERATTACKS

84%
of respondents agree that their cybersecurity teams feel pressured to prepare for the next cyberattack.

72%
agree the threat landscape is becoming more challenging, yet …

… ONLY **32%**
say their firm has a formal strategy to ensure cyber resilience.*

82% agree they could have mitigated some to all impact of the most significant cyber incident in the last 12 months if their teams were more prepared.

CYBERSECURITY TEAMS ARE INSUFFICIENTLY PREPARED FOR CYBERATTACKS

Over 80% don't think their cybersecurity team has the necessary skills to effectively respond to the next cyberattack.

64% agree that traditional cybersecurity training methods (e.g., certifications, video trainings, classroom instruction) are insufficient to ensure cyber resilience.

LACK OF TALENT HOLDS CYBERSECURITY TEAMS BACK

The top challenges firms face when maintaining cyber resilience are people related:

- Lack of team resources
- Lack of security expertise
- Inability to hire for desired skill sets
- Lack of bandwidth to train and upskill
- Lack of strategy to focus on training and upskilling

FIRMS ARE INVESTING IN NEW APPROACHES TO BUILD AND PROVE CYBER CAPABILITIES

70% agree their firm is making investments to improve in-house cybersecurity team training in the next year.

Over 60% are investing in the two most effective cybersecurity upskilling approaches:

1. Live simulations
2. Online training and upskill platforms

Base: 316 global decision-makers of cybersecurity training strategies
Source: A commissioned study conducted by Forrester Consulting on behalf of Immersive Labs, December 2022
*For the purposes of this study, cyber resilience is defined as the ability and confidence in a cybersecurity team's ability to prepare for and quickly detect, defend, respond, adapt, recover, and learn from a security breach or unexpected and unknown threats.

Read the full study