STRATIUUM

INSIGHTS

“ARE YOU AFRAID OF THE DARK (WEB)?”

The financial losses, regulatory scrutiny, and often irreparable reputational harm inherent in a successful cyber attack, can present a real threat to an organization’s business, and sometimes its very survival.

You need look no further than the seemingly endless string of media reports to recognize that cyber adversaries are relentless in developing new and nefarious ways to attack. While most boards and senior executives accept that the cyber threat is real, perhaps even inevitable, many struggle to orient traditional risk management practices towards enhancing the organization’s overall cyber resilience.

Increasingly, directors and senior executives are being held accountable for their organization’s cybersecurity posture

As Regulators retrospectively exact significant penalties from firms for past breaches, and we see an uptick in shareholder derivative actions filed against directors and officers for their alleged breach of fiduciary duties, cyber risk management, strategy, and resilience need to be more prominent topics in the boardroom.

Whether as a short, focused workshop to consider the impact of potential threat scenarios and enhance situational awareness, or as a war game designed to emulate the pressure of a real cyber attack, well orchestrated simulations are a highly effective - and crucially, practical - technique to help business leaders build the insight, culture, and resilience they need to evolve their cyber risk maturity.

How confident are you in your role as custodian of the brand?

An organization's brand is a priceless asset. Beyond equipping boards and executives with the capabilities they need to preserve the confidence of customers, regulators and shareholders should a cyber attack occur, simulations can also clarify the true nature of the organization's threat exposure and provide greater visibility into how well prepared the organization is to limit the impact to its bottom line and market standing.

Situational Awareness

Do you know what assets and information are most at risk? Who from? Can you anticipate how an attack might unfold? What early warning indicators or triggers should you be alert to to avert potential threats before they emerge?

Planning Strategies

Have you accurately gauged how a cyber attack could impair your organization? Are you focused on, and investing in, the right things? Do you have plans and strategies in place to minimize any adverse impacts?

Leadership

Do you have strong leadership to make strategic decisions and prioritize actions in the wake of a breach? Is governance clearly defined? Are you clear on your fiduciary and regulatory obligations?

Effective Partnerships

Do you have people outside your organisation you can rely on to support you should a breach occur? Are arrangements to do this already in place?

Internal resources

Do you have the right organizational talent? Can they be mobilized quickly to contain damages? Are roles and responsibilities clear should a breach occur?

Proactive posture

Could you communicate appropriately and transparently to all stakeholders? Have your strategies, plans and processes been evaluated? How well would you perform if you were breached?

The decisions you make and strategic actions you take in response, can make the difference between survival and demise

Simulations have long been conducted by the military and armed forces to test capabilities, surface vulnerabilities and improve their leaders' preparedness to take strategic actions during events that are not easily predicted.

Moves and counter moves are played out to immerse participants in the experience of a real cyber event. Designed around realistic threat scenarios, this dynamic technique brings critical insights into the adequacy and robustness of the organization's response strategies, tactical plans and ability to anticipate potential cyber threats.

A tried and tested technique to build the insight, culture and resilience needed to evolve the organization's overall cybersecurity posture

The complexity of the simulated scenario is tailored to address specific business objectives; the format and intensity can vary depending on the purpose and extent of organizational participation and experience.

Get broadly educated

WORKSHOP | At one end of the continuum, workshops focus discussion around specific threat scenarios to heighten situational awareness and support the development of cybersecurity strategies and plans. They can also be used to help business leaders develop a common language, identify critical assets and drive out false assumptions.

Rehearse and assess plans

TABLETOP | Tabletop exercises simulate an environment that allows participants to practice functioning in the capacity they would were they responding to a real event. These simulations often focus on sharpening specific skills, for example, rehearsing decision-making and communication protocols, or testing specific response plans and processes.

Evaluate capabilities

WAR GAME | At the end of the continuum, war games immerse participants in the pressure of a real and evolving attack, and often involve multiple layers of an organization. The simulation is played out real time and is designed to stress an organization's ability to react to a cyber event as it unfolds, building muscle memory and giving participants the opportunity to hone their response reflexes.

Either as a standalone exercise or as part of a progressive program, simulations yield critical insights into an organization's resiliency strengths, vulnerabilities and preparedness to withstand and recover from a cyber attack.

Navigating the cyber threat landscape

Cybersecurity risks are growing, both in their prevalence and in their disruptive potential. As the world becomes more complex and interconnected, today's business leaders are under great pressure to rethink how they manage risk and build resilience.

Cyber resilience extends beyond an company's ability to withstand and recover from a cyber event. A truly resilient organization has the foresight and situational awareness to avert potential threats before they emerge, and an ability to adapt and prosper, turning the cyber challenge into a source of strategic opportunity.

Meeting the cyber threat with greater fortitude

Simulations bring much needed context and education around what is an opaque and evolving threat, helping organizations prioritize their cybersecurity investments and align efforts with strategic business goals.

CONTACT

To discuss your organization's cyber challenges, or to find out more about our Cyber Resilience solutions, please contact:

Cath Stewart
Managing Principal
New York, NY

✉ cstewart@stratiuum.com

About STRATIUUM

We are a specialized risk advisory firm built to help clients navigate today’s complex operating environment and turn their most critical business challenges into sources of strategic opportunity. Our focus is on emerging strategic risks that pose serious threats to an organization’s bottom line, growth prospects and market standing. Against the backdrop of today’s nefarious threat landscape, we help our clients identify and protect their organization’s critical assets, reduce the impact of a cyber event and align security investments with risk priorities. For more information about our organization and solutions, please visit **stratiuum.com**

This article contains general information only and is not intended to be relied upon as professional advice or services. Before making any decisions, or taking any actions, that may affect your business, you should consult your professional advisors.