

# PREVENTION!

WHEN IT COMES TO CYBER RESILIENCE, RESPONSIBILITY RESTS WITH A FIRM'S BOARD. ALL BOARD MEMBERS SHOULD BE FAMILIAR WITH THE RISKS OF CYBER BREACHES, WITH AT LEAST ONE BOARD MEMBER TAKING RESPONSIBILITY FOR THE FIRM'S CYBER RESILIENCE PROGRAMME.

There are many resources available to board members to help them understand cyber threats and assess how prepared their firms are for them. Board members aren't expected to be cyber resilience experts, but they need to be able to ask the right questions and know when they are getting the wrong answers.

## GOVERNANCE



- » What kind of expertise about cyber security exists on the board of directors?
- » Does the board understand the firm's total risk exposure from a cyber attack perspective (e.g. financial, third parties, legal, customer risk, reputation), including cyber insurance coverage?
- » Does the board have access to independent experts?

## RISK ASSESSMENT



- » Does the firm have a robust, well documented programme to monitor the exposure and report on cyber risks?
- » How frequently are cyber security risk assessments conducted (quarterly, annually, etc.)?
- » How does the firm evaluate the effectiveness of its cyber risk programme?

## OUTSOURCING



- » What has the firm done to protect itself against third-party cyber risks?

## RISK MITIGATION



- » What authentication methods are used to control access to systems and data?
- » What training does the firm have in place for employees?

## RESPONSE



- » How many times was the firm the target of an attack during the past year, and how far did the most serious attack reach in the system? Were communication and escalation procedures followed?

## FINANCIAL IMPACT



- » Has the firm assessed the potential financial impact of an interruption caused by a cyber attack? Is it possible to quantify the impact?

## TESTING



- » Does the firm perform vulnerability assessments and/or penetration tests?

## RESOURCES:

- » **NCSC:** Cyber Security Toolkit for Boards
- » **FCA:** Cyber Security – Industry Insights
- » **IA:** Building Cyber Resilience in Asset Management
- » **NASAA:** Cybersecurity Checklist for Investment Advisors
- » **The Pensions Regulator:** Cyber Security Principles for Pension Schemes
- » **IOSCO:** Cyber Task Force – Final Report
- » **International Standards:** ISO 27001 and ISO 27002
- » **ECB:** Cyber resilience oversight expectations for financial market infrastructures
- » **World Economic Forum:** Advancing Cyber Resilience - Principles and Tools for Boards

