MARSH RISK CONSULTING

Cybersecurity Consulting
and Advisory Practice

CYBER INCIDENT AND BREACH RESPONSE PREPAREDNESS

Cyber threats and related breach events are a fact of life for today's organizations. Almost every business relies on the internet or utilizes connected technologies in some way in their operations or to generate revenue.

A well-developed Cyber Incident and Breach Response (CIBR) plan is critical to business resilience and functions as an important risk mitigation tool. While essential to any company's enterprise cybersecurity program and IT risk management plans, a CIBR plan on its own is not enough.

Organizational leaders and response team members should participate in detailed tabletop exercises to clearly understand their roles and CIBR plan processes. These exercises should have both a technical component to help validate the technical aspects of the CIBR plan and expose the senior leadership team to the types of events and decisions that they will be required to make in a real world cyber incident. Additionally, leaders must seek to leverage the lessons learned from these exercises to continually refine and mature their CIBR plan.

Marsh Risk Consulting's (MRC) CIBR preparedness services provide plan development and training support tailored to the key cyber threats your organization faces. Our experts work with you and your cybersecurity stakeholders to deliver:

- A cyber incident and breach response plan in line with current best practices and your organization's specific cyber risk profile.
- Supporting documents, forms, and templates to further an organized and measurable response.
- Workshops and reviews to test whether the final plan is current, effective, and efficient.
- Tabletop exercises designed to equip senior managers and incident responders with the knowledge they need to effectively respond to cyber incidents.

Who it's for

- Organizations seeking guidance and professional cyber expertise support with their efforts to comprehensively prepare for cyber incidents and mitigate operational and bottom line impacts.

What you get

- A tailored CIBR strategy, plan, and identification of training needs.
- A CIBR plan that includes vetted internal and external resources with clear support roles.
- Workshops and plan reviews geared towards finalizing a plan that is effective and efficient.
- Checklists, forms, and templates to support a measurable and organized response.

OUR THREE-PHASE APPROACH TO CYBER INCIDENT AND BREACH RESPONSE PREPAREDNESS

PHASE I:

EXAMINE AND DISCOVER CRITICAL ORGANIZATIONAL ELEMENTS

- Develop the CIBR preparedness strategy, goals, objectives, and governance.
- Identify key CIBR stakeholders and team members within the organization through interviews and other discovery methods.
- Conduct a CIBR workshop to identify:
  - Team roles, responsibilities, and requirements.
  - Key internal and external resources.
  - Event coordination, information reporting, and tracking guidelines along with associated frequency/timelines.
  - Regulatory requirements unique to specific business operations and geographies.

PHASE II:

DEVELOP PROCESSES AND PROCEDURES

- Identify CIBR external partner support.
- Establish logistical details including where the team will convene and contact information for relevant internal stakeholders and external partner resources.
- Finalize CIBR event response, prioritization, and escalation processes.
- Formalize and create forms and templates in relation to CIBR information reporting requirements and tracking guidelines.
- Develop CIBR After Action Review and Lessons Learned templates to capture process improvement opportunities and key point summaries for leadership following an actual event or training exercise.
- Conduct a CIBR event dry run with the CIBR team to review processes and procedures prior to Phase III.

PHASE III:

TEST, TRAIN, AND REFINE

- Conduct a cybersecurity tabletop exercise review or walkthrough of a cyber incident or breach event to validate the CIBR preparedness plan and processes. Revise and refine the plan and process as needed.
- Implement an annual CIBR preparedness exercise program with the objective of maintaining a minimal level of CIBR team proficiency.
- Define and document periodic review to assure that plan and processes remain current and address changes within the organization or in the external cyber threat environment.

WHY MARSH?

Marsh helps clients review and define cyber risk as an opportunity for performance improvement and optimization of cyber risk capital efficiency to enable confident, strategic risk taking that supports business growth.

We aim to help you reduce your concerns about cyber risk, so you can focus on your business.

To learn more about our cybersecurity consulting capabilities, please contact your local Marsh representative.

THOMAS FUHRMAN
Managing Director
+1 703 731 8540
thomas.fuhrman@marsh.com

JAMES HOLTZCLAW
Senior Vice President
+1 202 297 9351
james.holtzclaw@marsh.com

JOHN NAHAS
Vice President
+1 202 297 9048
john.nahas@marsh.com