
AMCHAM
OMAN
PRESENTED BY:
كينيدز
Kennedys
IN COLLABORATION WITH:
MARSH
AI, PERSONAL DATA & LIABILITY
WHAT BUSINESSES NEED TO KNOW NOW
Navigating Legal Risk, Regulatory Accountability and Operational Resilience

Key Takeaways from Marsh:

- The cyber risk landscape is continuously evolving, presenting organisations with growing challenges across data regulation compliance, operational procedures, security control deployment, budget allocation, incident response and worst-case-scenario planning.

- Cyber insurance is designed to complement an organisation's cyber posture by transferring risk and helping to reduce the impact of losses from profit, incurred costs of recovery, damaged reputation, operational resilience and legal obligations to minimise the risk of further fines or penalties.

- Marsh are committed to help you Understand, Measure, Managed and Respond to your cyber risks and incidents - providing expert guidance at every stage.

- To undergo a comprehensive assessment of your organization’s security posture, please reach out to Hannah.parry@marsh.com to begin the Marsh CSA (Cyber Self-Assessment)

MARSH

2026

AI, Personal Data and Liability

Cyber Insurance Strategy

Marsh Cyber Practice MENA

Agenda

1. Understanding Your Requirements, Risk & Exposure
2. The Role of Cyber Insurance
3. Global CIM
4. Our Approach to Risk Management
5. Case Study
6. Appendix A:
    a) Who are We
    b) State of the Market
    c) Claims Process

MARSH

Understanding Your Requirements, Risk & Exposure

01

MARSH

Key Cyber Risks in your various industries

Cyber risks are a growing concern as we are all increasingly reliant on digital systems for operations, security, and customer experience across a number of industries...

Real Estate: Common risks include Business Email Compromise (BEC) scams that trick parties into wiring funds, ransomware attacks that lock critical systems/information causing operational downtime and lost business opportunities , and data breaches exposing personal and financial information of clients/third parties.

Construction: OT is a prime target for cyberattacks and can cause system failures, safety hazards, property damage and operational downtime - delaying projects and incurring a range of extra costs. Firms face risks like data theft, fraudulent payments, and compromised supply chains, all of which can undermine project timelines and damage reputations.

Healthcare: The industry faces critical cyber risks that threaten patient safety, data privacy, and operational continuity. Cyberattacks such as ransomware can disrupt medical devices and hospital systems, leading to treatment delays and compromised care**.** Data breaches expose sensitive patient information, resulting in identity theft, regulatory penalties, and loss of trust.

Hospitality: Cyberattacks like ransomware and data breaches can lead to system outages, lost bookings, and exposure of sensitive personal and payment information. These incidents result in financial losses, regulatory fines, and significant reputational damage, undermining customer trust.

Energy: A cyber event here can disrupt critical infrastructure and threaten national security. Targeting OT could cause power outages equipment damage and significant safety hazards, leading to regulatory penalties, harm to reputation, downtime and substantial financial loss.

Financial Institutions: The financial institution industry is a prime target for cyberattacks due to the sensitive financial data and assets it manages. Cyber risks such as data breaches, ransomware, and fraud can lead to significant financial losses, regulatory penalties, and erosion of customer trust.

MARSH

2026 Cyber Risk Environment – MENA Perspective

Key trends

Global Cyber Events & Trends

- **Rise in Ransomware Attacks impacting full Supply chain:** Scattered Spider / M&S and JLR, Ingram Micro, Heathrow airport)
- **Growing Systemic Cyber Events & Supply Chain Vulnerabilities:** Cloud outages **and supply chain attacks rose 136%** in early 2025, exposing critical dependencies on global IT vendors.
- **Several global systemic events were recorded in 2025**: Azure, Cloudflare and AWS Outage and Salesforce & Oracle Data breach
- **Expanding Attack Surface from Digital Transformation & AI**: Rapid AI adoption broaden the attack surface, enabling both enhanced defense and sophisticated attacks.

New Data Privacy Regulations Rolled out in GCC

- **KSA:** PDPL Regulation in place since Sept 24, incidents to be reported to SDAIA, fines applicable for Personal Data Misuse**,** **48 fines issued in 2025**
- **UAE:** DIFC & ADGM Incidents to be reported, fines being issued regularly. PDPL federal decree in place, **Executive regulation expected soon**
- **Oman, Bahrain, Qatar:** Data Privacy Laws incorporating Data breach notification requirements and fines in place.
- **Globally:** GDPR related fines are growing in 2025:
  - TikTok – USD 6000m,
  - Shein – USD 170m,
  - Google – USD 230m.

Cyber Trends in MENA

- **Notifications to Marsh: Several multi million dollars Cyber incidents in GCC**, across various sectors including Real Estate, Energy, Healthcare Financial Institutions and Retail / Distribution.
- Ransomware attacks: Ransomware attacks in MENA **surged by 80% in 2025**, with advanced tactics like double extortion increasing operational risks.
- **Cost and Frequency of Cyber incidents Rising**: more frequent and costly, with an average ransomware claim reaching **$1.72 million** and data breach costs in Middle East ranking 2nd globally, at 7.3 Million USD on average for large corporates, driven up by new regulations.

MARSH

Sources: Crowdstrike 2025 Threat Hunting report, IBM 2025 Cost of Data Breach, UAE Cybersecurity Council, MMC Cyber Analytics Center; Norton Rose

Data Breaches in the Region

Example Breaches across GCC

Company Type: Energy company
Date of Breach: December 29, 2019

Compromise: Saudi security experts believe the company was originally compromised through its VPN servers in the summer of 2019, exploiting remote execution bugs in high-end commercial servers. The attackers escalated to domain admin level, then deployed the Dustman wiper malware.

Impact: The malware attack was partially successful, affecting only a certain module of its extensive network. The company was able to detect and contain the malware and continued normal services after the attack. Reports at the time cited over 2,000 damaged computers, with losses described as amounting to millions. No regulatory fine disclosed. Losses "amounting to millions" reported in Bahraini press but unquantified

Company Type: Healthcare benefits company
Date of Breach: 2021

Compromise: Hackers exploited compromised credentials to gain access via a remote access application. The absence of multi-factor authentication is suspected to have been a key enabling factor. Once inside, the attackers moved freely through the network, indicating they had ample time to exfiltrate large volumes of data.

Impact: Hackers obtained 201 GB of data and published half of it. The leaked information included patient names, phone numbers, credit card data, admission diagnoses, COVID-19 test results, medical records, and clinical notes on patient conditions. The security team received information about the breach very late, as the notification email had gone to spam.
Financial Consequences:

No regulatory fine has been publicly disclosed under Saudi Arabia's PDPL (which came into force in 2022). The company contacted KSA authorities and affected patients. Credit card data exposure creates potential fraud liability. Exact financial impact undisclosed.

Country of Breach

Data Breaches in the Region

Example Breaches across GCC

Company Type: Supermarket
Date of Breach: 2023–2024

Compromise: The leading UAE retail chain fell victim to a data breach in which over 200,000 customer records were compromised, including personal details such as email addresses and phone numbers. The specific attack vector was not publicly disclosed.

Impact: Over 200,000 customer records exposed, including personally identifiable information. No financial data was reported as compromised. Reputational damage in a highly competitive retail sector.

Company Type: Government-owned energy company
Date of Breach: November 2024

Compromise: Government-owned energy investment company headquartered in Muscat and operating across 17 countries, was listed as a victim by the Termite ransomware group in November 2024. Termite is believed to use generic ransomware TTPs including initial access via phishing, exploitation of vulnerabilities, or purchased credentials, followed by privilege escalation to take control of networks.

Impact: he group claims to have accessed and leaked confidential company data, potentially including sensitive operational or corporate files. Given their strategic role in Oman's energy, petrochemical, and infrastructure sectors, any compromise could pose risks to both business continuity and national energy security.

This breach occurred during Oman's PDPL transitional period - a similar breach occurring today could attract fines of up to **OMR 500,000** (~$1.3M).

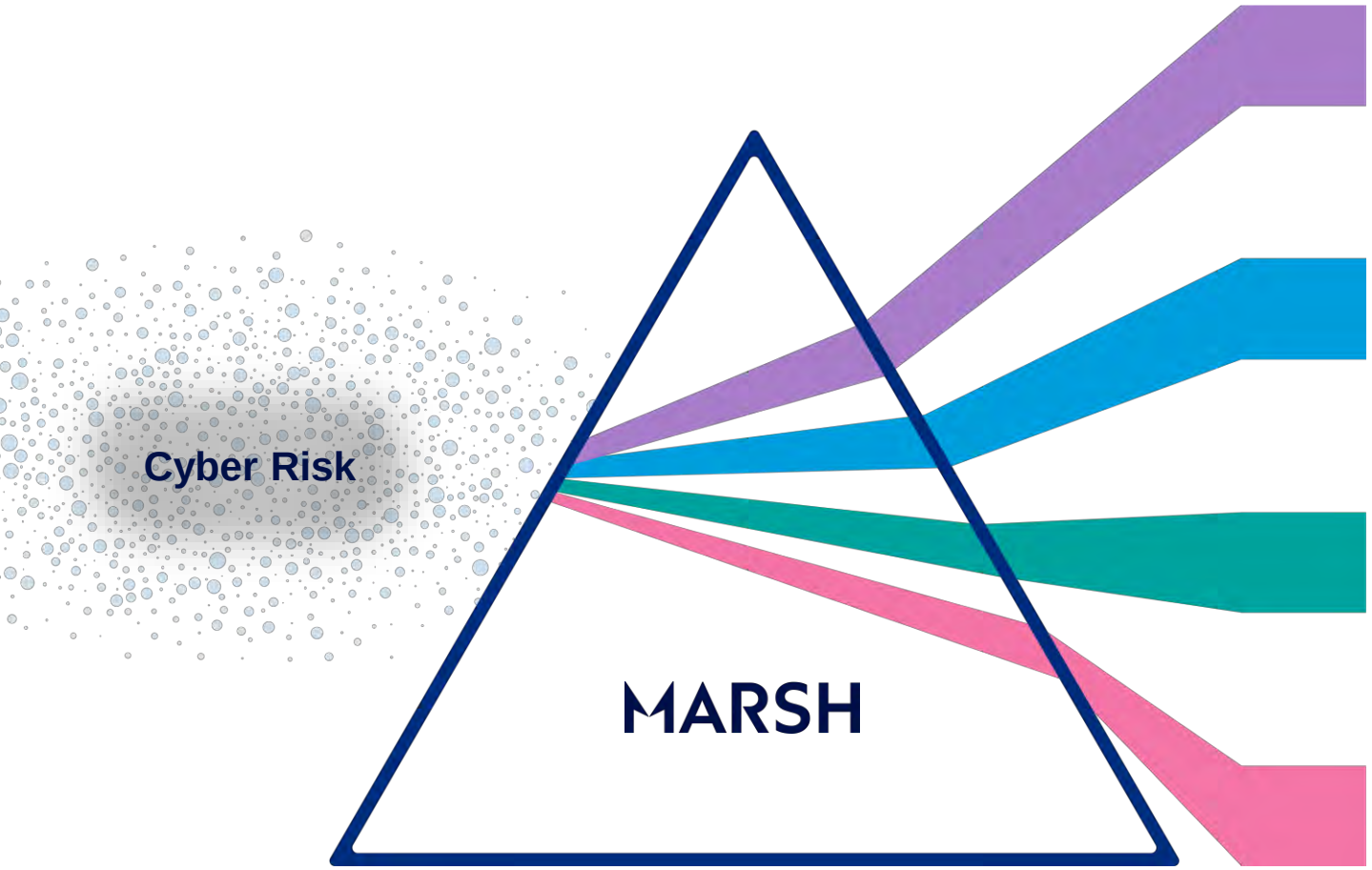
Country of Breach

The Role of Cyber Insurance

02

MARSH

Cyber Risk is Complex



Understand

You need to understand what's happening. We help you approach cyber risk with clarity and confidence.

Measure

You need to quantify your cyber risks. We use tools powered by risk intelligence.

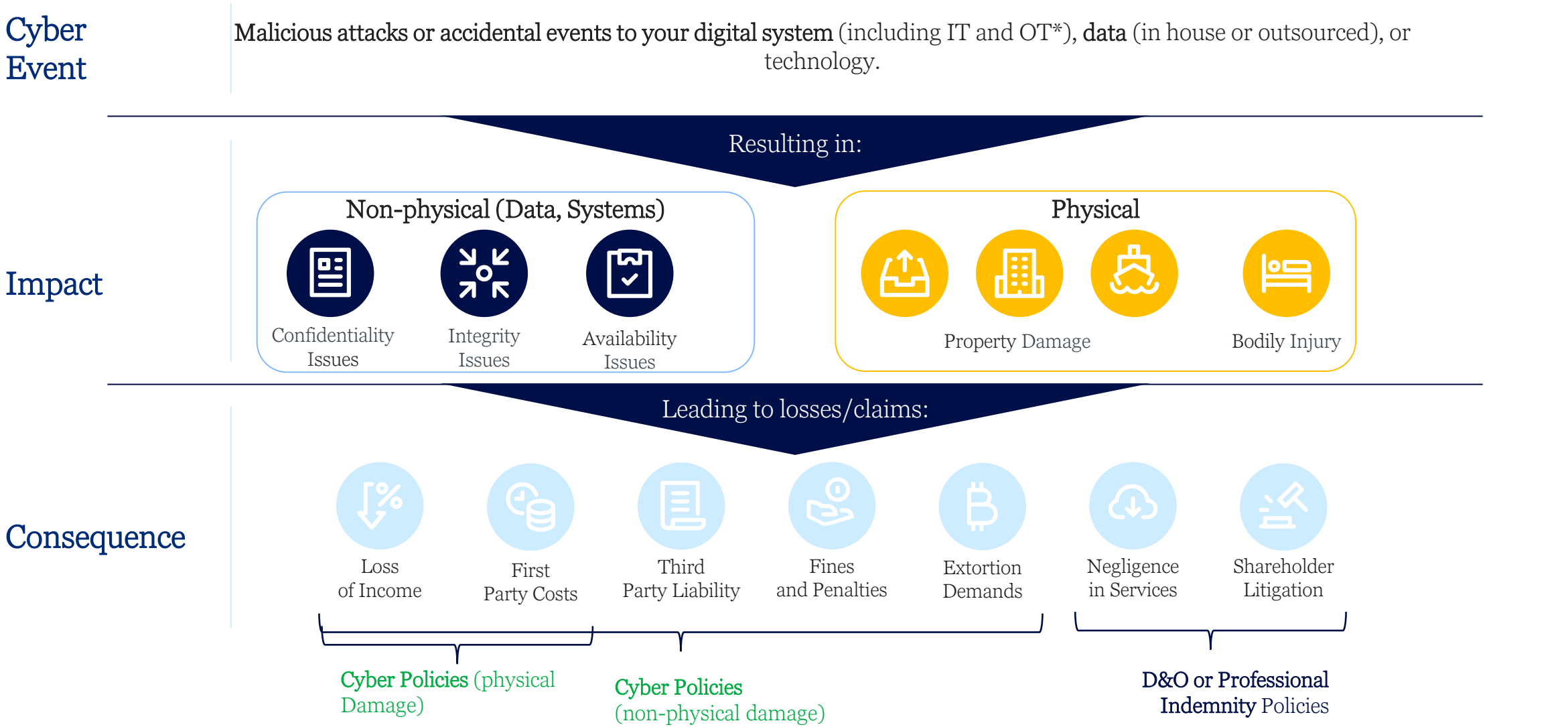
Manage

You need to protect your organization. We help you find the right balance between cyber security and insurance solutions.

Respond

You need to be prepared and respond. We help you respond and build resiliency.

Understanding the impact and consequences of a Cyber Event



*Operational Technology

Summary of Cyber Insurance Coverage

1st Party Costs
Triggered upon discovery of an event

Business Interruption
Loss of gross profit and increased cost of working resulting from a security event, including voluntary shutdown

Costs & Expenses
Costs and expenses incurred to:
- identify security event
- restore data and IT system
- maintain operability of IT system
- legal response to regulator / third party
- develop communication strategy

Cyber Extortion
Costs and expenses incurred, including digital currencies to prevent or to terminate the extortion threat

PCI-DSS Penalties
Costs and expenses incurred including direct monetary fines, penalties, assessed against the bank following a security event or data breach

3rd Party Liabilities
Triggered by a demand/lawsuit

Security Event or Breach of Confidentiality of Personal Data
Defence costs and financial consequences to a third party, following a security event or personal data breach

Multimedia Cover
Defence costs and financial consequences to a third party as a result of wrongful acts committed on multimedia channels

Personal Data Protection
Costs and expenses incurred in fulfilling legal and regulatory obligations following a personal data breach

Defence Costs and Penalties resulting from regulatory investigation
Defence costs and Financial penalties resulting from investigation following security breach or personal data breach

MARSH

Note: Above is intended for summary purposes and you may refer to the policy wording for full definitions, terms & conditions.

Global CIM

03

MARSH

Claims & Incident Management

How you respond makes all the difference

Prepare

Creating and testing IR plans reduces losses by $1.49 M on average – IBM Cost of a Data Breach Report 2023

- Marsh Central
- Incident response plan review and development
- Incident response vendor selection

Test

Well-practiced teams know their roles, responding quickly and effectively.

- Tabletop exercises & crisis simulations

Respond

A coordinated, holistic effort is vital for effective incident response.

- Marsh Central
- Active Incident Response (AIR) support

Recover

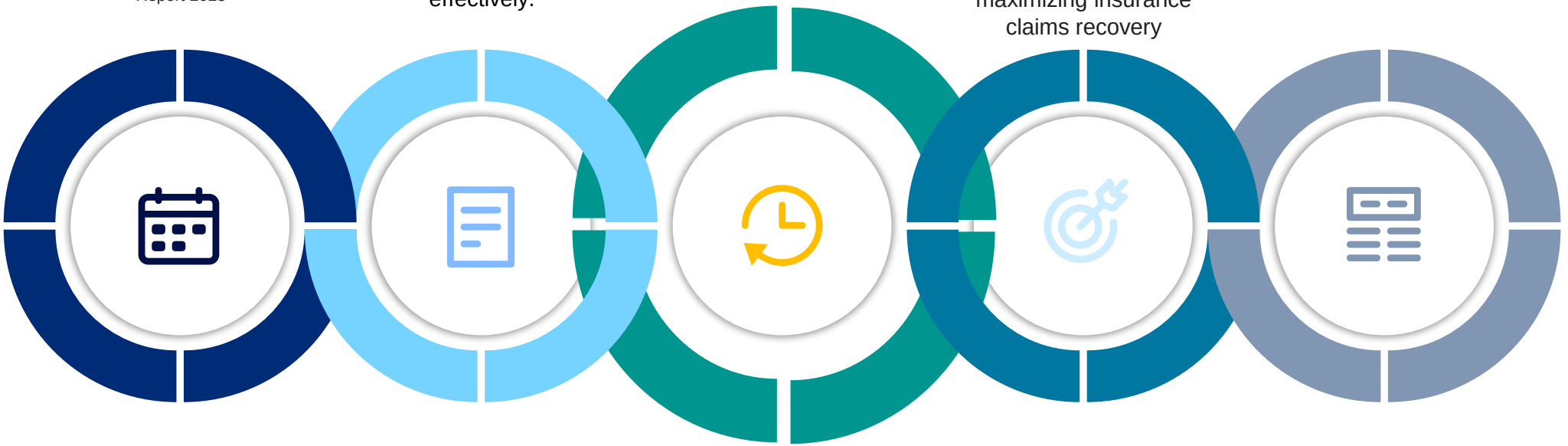
Expert support ensures proactive navigation of cyber claims complexity, maximizing insurance claims recovery

- Claims preparation/ forensics accounting
- Claims advocacy

Enhance

Convert learnings and challenges into opportunities for growth

- Resilience Roadmap Development



MARSH

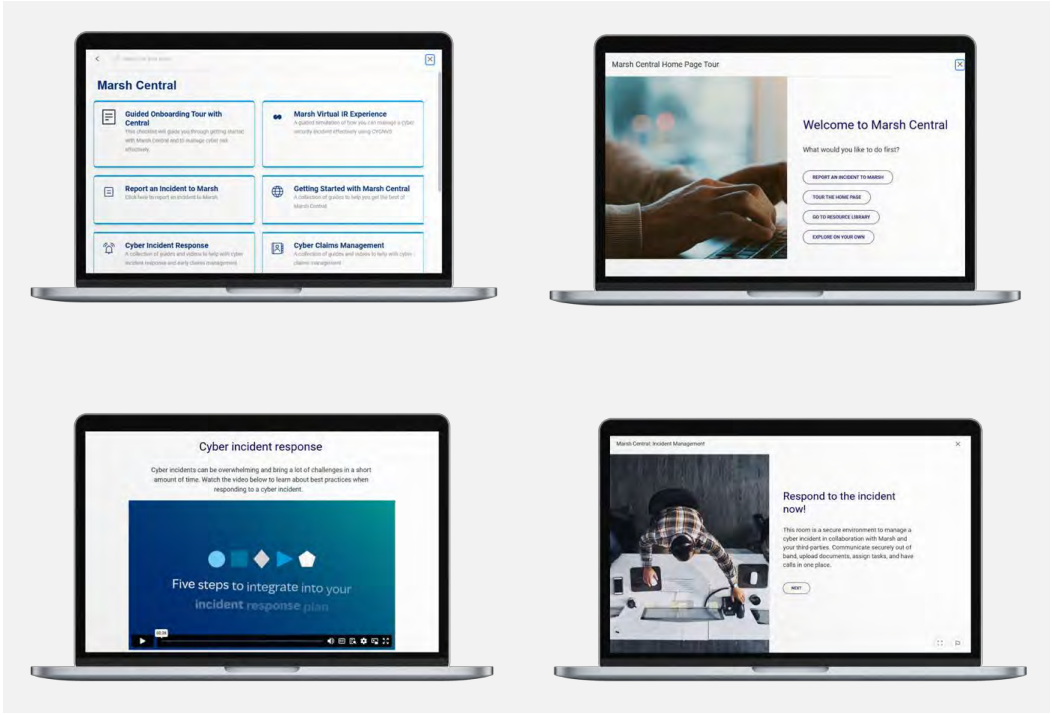
Marsh Central

Our innovative claims and incident management platform

We are pleased to announce that you now have access to Marsh Central, powered by CYGNVS. Marsh Central is an innovative platform designed to help clients with their claims and incident management.

With a user-friendly interface, the platform serves as a comprehensive resource for preparation, response, and recovery. Once registered, you will have access to essential tools and information all in one place, allowing your team to:

- **Communicate and collaborate with key stakeholders:** With incidents occurring when they are least expected, it's important to have a secure, out-of-band global communication tool available at all times.
- **Access incident response plans at their fingertips:** With Marsh, you can store and easily access critical documents off-network, such as an incident response plan.
- **Manage and document incident and claims activity:** During and after an incident, the ability to easily and accurately collect incident information, including for a potential audit, is critical.
- **Review best practices and tips:** Access a curated collection of articles, tip sheets, and videos, designed to help organisations effectively manage claims and incidents.
- **Practice managing cyber incidents with our virtual IR experience:** Work your way through key decision points and consider what support you may need to engage in a cyber incident.



By enabling seamless communication and collaboration with key stakeholders, the platform will support incident preparedness, provide a more coordinated response to incidents, and facilitate a smoother recovery.

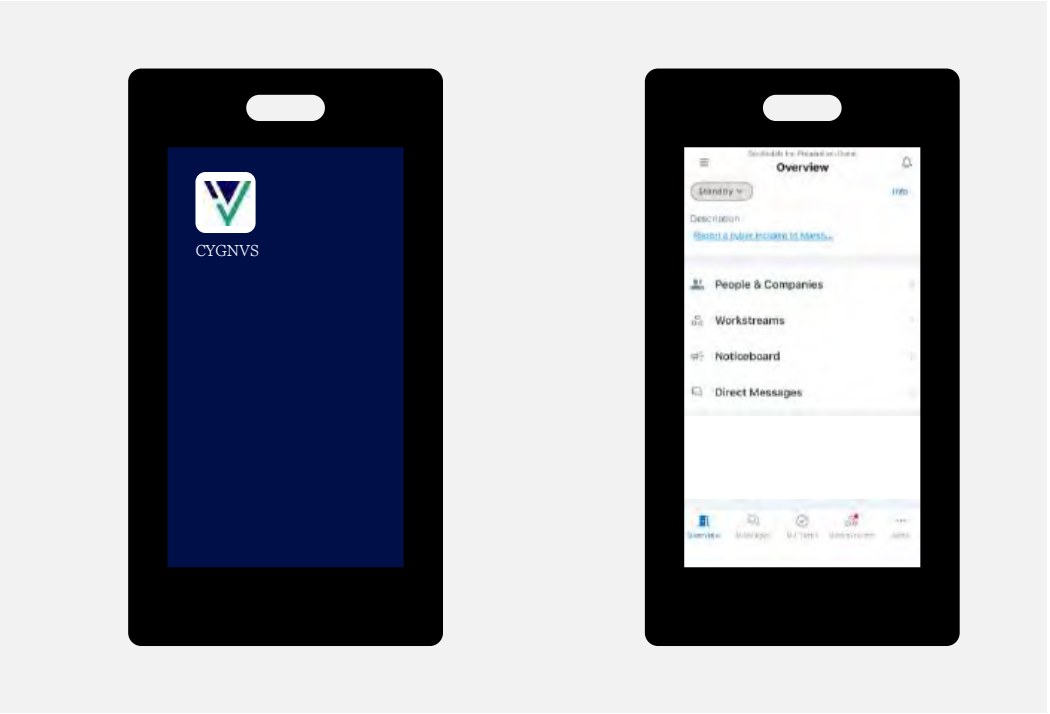
Marsh Central

Our innovative claims and incident management platform

We are pleased to announce that you now have access to Marsh Central, powered by CYGNVS. Marsh Central is an innovative platform designed to help clients with their claims and incident management.

With a user-friendly interface, the platform serves as a comprehensive resource for preparation, response, and recovery. Once registered, you will have access to essential tools and information all in one place, allowing your team to:

- **Communicate and collaborate with key stakeholders:** With incidents occurring when they are least expected, it's important to have a secure, out-of-band global communication tool available at all times.
- **Access incident response plans at their fingertips:** With Marsh, you can store and easily access critical documents off-network, such as an incident response plan.
- **Manage and document incident and claims activity:** During and after an incident, the ability to easily and accurately collect incident information, including for a potential audit, is critical.
- **Review best practices and tips:** Access a curated collection of articles, tip sheets, and videos, designed to help organisations effectively manage claims and incidents.
- **Practice managing cyber incidents with our virtual IR experience:** Work your way through key decision points and consider what support you may need to engage in a cyber incident.



By enabling seamless communication and collaboration with key stakeholders, the platform will support incident preparedness, provide a more coordinated response to incidents, and facilitate a smoother recovery.

Our Approach to Cyber Risk Management

04

MARSH

Complimentary Digital Tools to Make More Informed Decisions

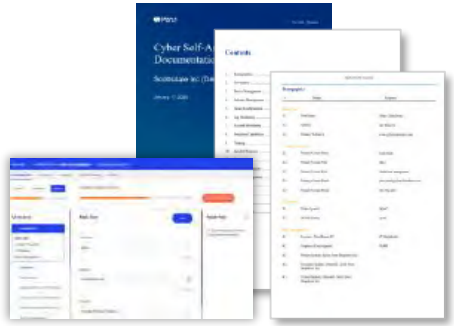
Completely free of charge, the Marsh Cyber Self-Assessment is a next-generation diagnostic tool that incorporates the NIST cybersecurity framework that provides a single, shared view of your risk across 16 categories and helps to rank your overall cyber maturity

Gaining Access to CSA

Provide your Marsh contact with user details who is going to access and complete CSA. Typically, users are from Cybersecurity, IT/OT divisions. We can grant access to as many users, within 48 hours of request followed with login instructions.

CSA Platform

Click Submit to Marsh



Cyber Self Assessment, Marsh's underwriting tool provides 360 look of your organisation's both IT & OT capabilities and generate an underwriting report

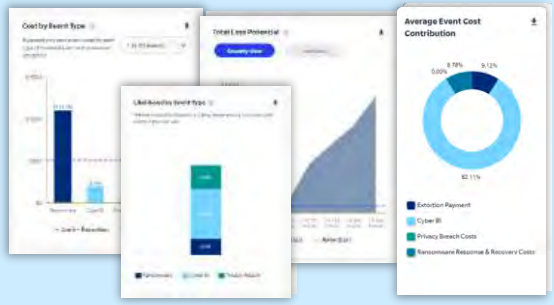
Top Cybersecurity Controls Analysis

TCC analysis is performed on the 12 key controls on IT environment, providing you how cyber insurers' will perceive your cyber risk.

Peer Maturity & Benchmark Reports

Reports produced follows the NIST Cybersecurity Framework.

Cyber Event Cost Quantification Insights



We then utilize a predictive analysis to provide to you with potential cost impact of a non-physical cyber event can give your organisation.

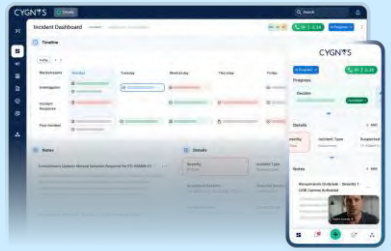
Cyber Insurance Program Peer Benchmarking

Our Cyber Benchmarks help organisations make informed decision regarding their Cyber Non PD program limit & deductibles.

Cyber Threat Report

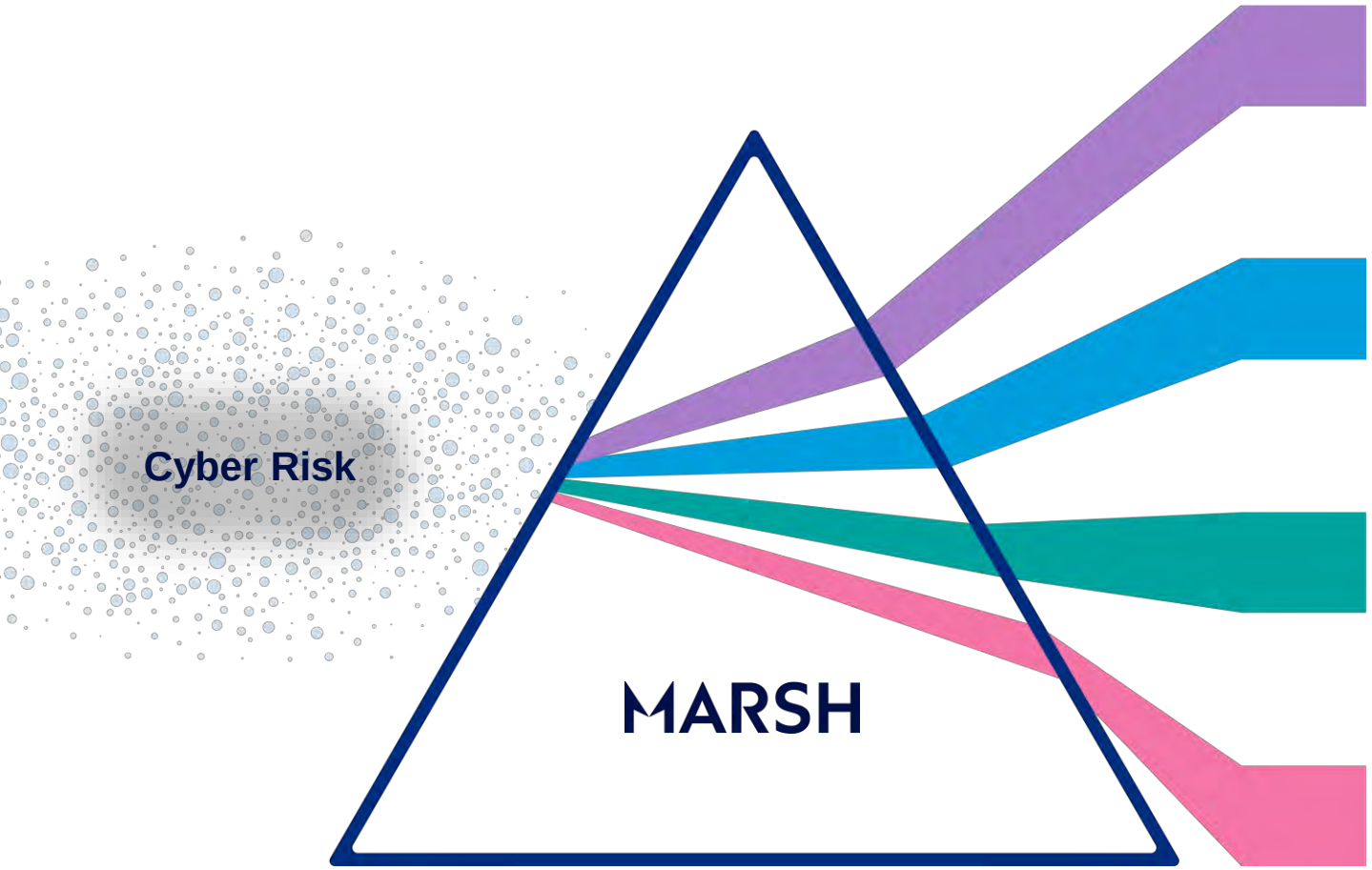
BitSight and Security Scorecard: External threat assessment of your firm's operational footprint and technical vulnerabilities. Searchlight: provides threat intelligence insights into dark web sources

Marsh Central Onboarding



Post placement Marsh Central onboarding is done

Cyber Risk is Complex



Understand

You need to understand what's happening. We help you approach cyber risk with clarity and confidence.

Measure

You need to quantify your cyber risks. We use tools powered by risk intelligence.

Manage

You need to protect your organization. We help you find the right balance between cyber security and insurance solutions.

Respond

You need to be prepared and respond. We help you respond and build resiliency.

Top Cybersecurity Controls

How did X score?

	Key Controls	Insurer Perception
1	MFA controlled access for remote access & admin / privileged access	
2	Endpoint Detection and Response (EDR)	
3	Secured, encrypted and tested backups	
4	Privileged Access Management (PAM)	
5	Email filtering and web security	
6	Patch management and vulnerability management	
7	Cyber Incident Response planning and testing	
8	Cybersecurity awareness training and phishing testing	
9	Hardening techniques including Remote Desktop Protocol (RDP) mitigation	
10	Logging & Monitoring / Network Protections	
11	End-of-life systems replaced or protected	
12	Vendor / Digital Supply Chain Risk Management	

Note – Full reports available

The overall maturity rating is on a scale from 1 (least mature) to 4 (most mature). The Marsh Cyber Self-Assessment rating for X is 3.0, indicating a mature cybersecurity program with some cyber-resilient characteristics.

Identify

Protect

Detect

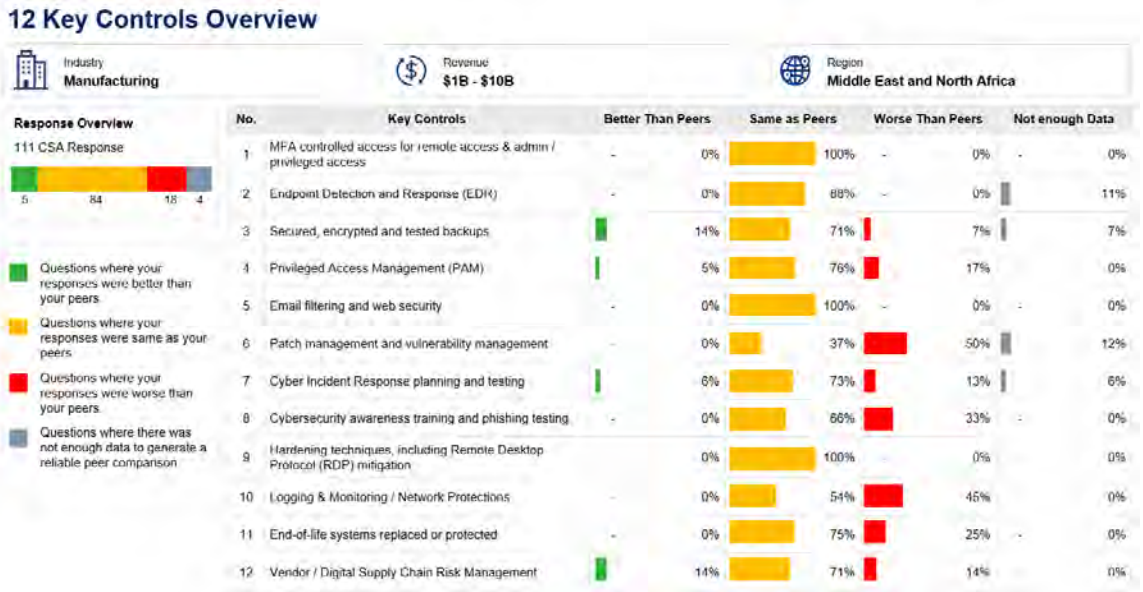
Respond

Recover

Peer Benchmarks

Compare your Key Controls maturity vs. peers

Peer Key Controls Benchmarking



12 Key Controls Overview

Industry: Manufacturing | Revenue: $1B - $10B | Region: Middle East and North Africa

Response Overview

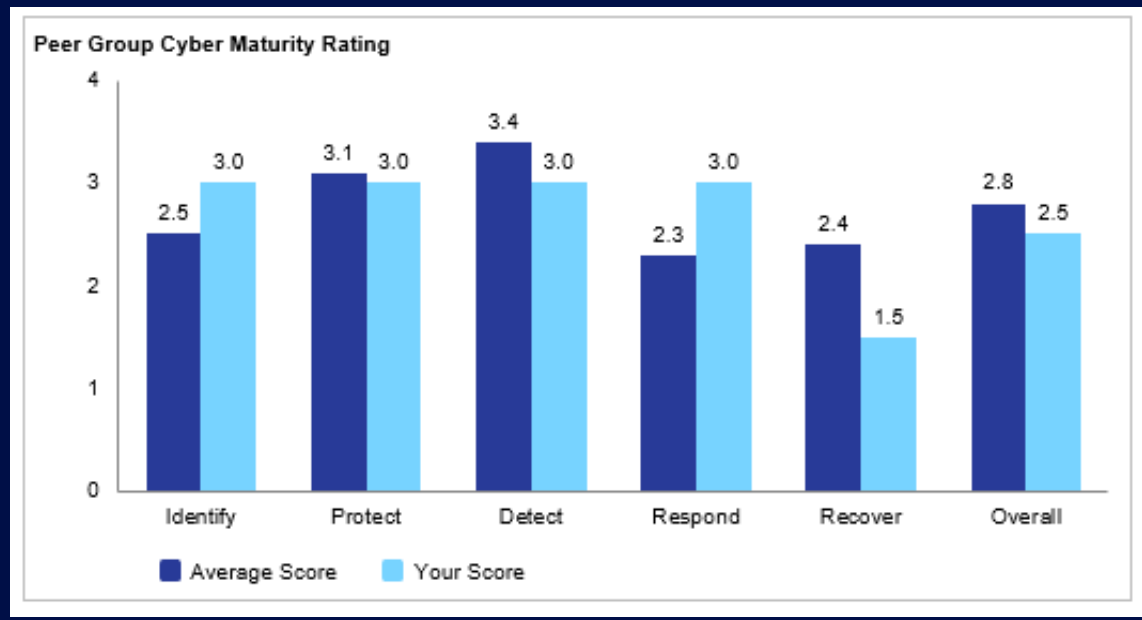
111 CSA Response

5 | 84 | 18 | 4

- Questions where your responses were better than your peers
- Questions where your responses were same as your peers
- Questions where your responses were worse than your peers
- Questions where there was not enough data to generate a reliable peer comparison

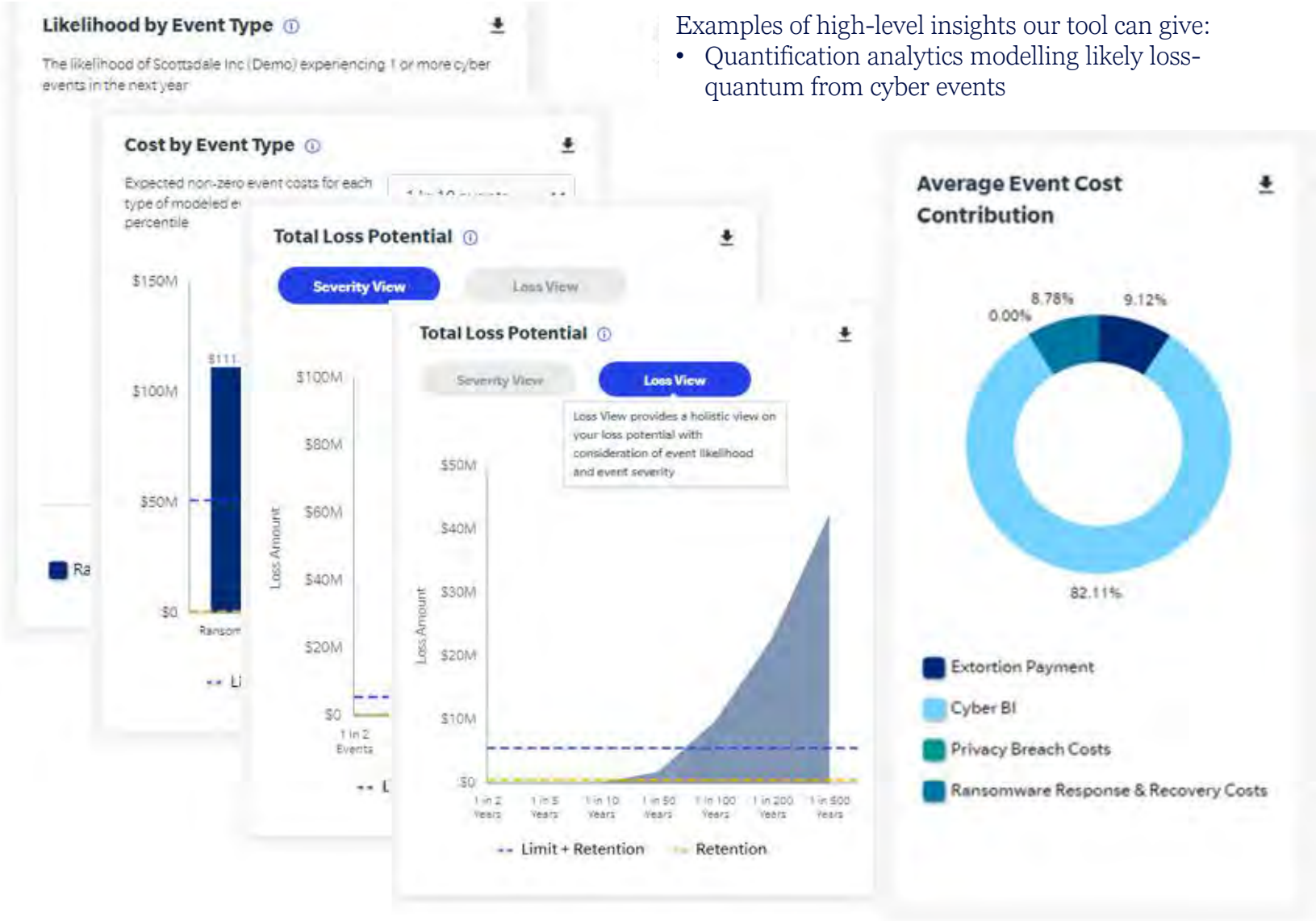
No.	Key Controls	Better Than Peers	Same as Peers	Worse Than Peers	Not enough Data
1	MFA controlled access for remote access & admin / privileged access	- 0%	100%	- 0%	- 0%
2	Endpoint Detection and Response (EDR)	- 0%	88%	- 0%	11%
3	Secured, encrypted and tested backups	14%	71%	7%	7%
4	Privileged Access Management (PAM)	5%	76%	17%	0%
5	Email filtering and web security	- 0%	100%	- 0%	- 0%
6	Patch management and vulnerability management	- 0%	37%	50%	12%
7	Cyber Incident Response planning and testing	6%	73%	13%	6%
8	Cybersecurity awareness training and phishing testing	- 0%	66%	33%	- 0%
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	0%	100%	0%	0%
10	Logging & Monitoring / Network Protections	- 0%	54%	46%	0%
11	End-of-life systems replaced or protected	- 0%	75%	25%	- 0%
12	Vendor / Digital Supply Chain Risk Management	14%	71%	14%	0%

Peer Maturity Rating Benchmarking



High-Level Cyber Quantifications

The Blue [i] quantification tool plays a huge part in facilitating this and leverages our powerful data and analytics tools and industry benchmarking. It helps clients gain insight into limits they should consider.



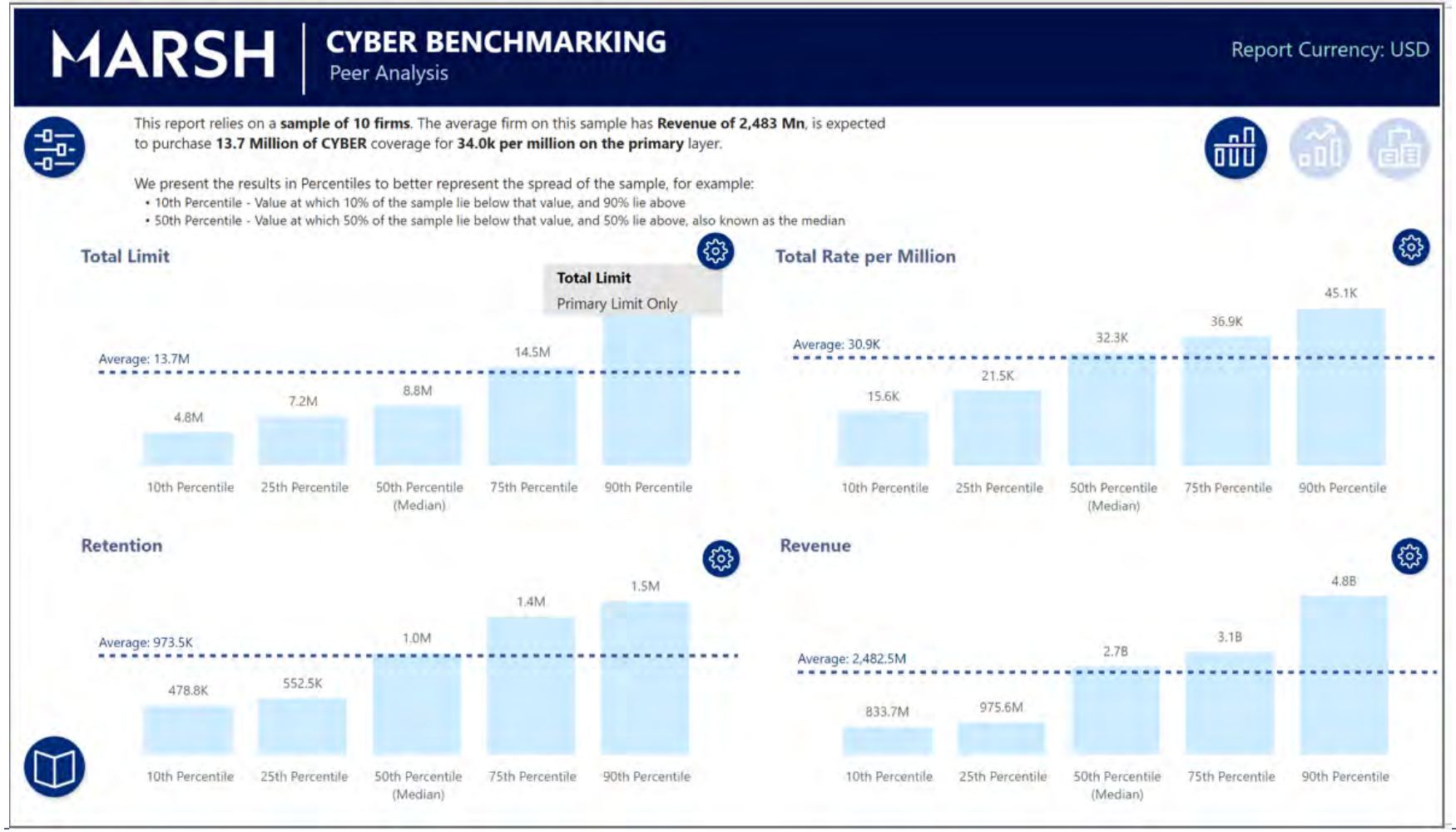
Examples of high-level insights our tool can give:

- Quantification analytics modelling likely loss-quantum from cyber events

Cyber Benchmarking

Estimates based on benchmarking

Our global reach allows us to benchmark Cyber limits for international companies via the Marsh's Global Benchmarking tool. We set out a sample below to better inform RAM of purchasing trends for similar organisations.



The benchmarking diagram as shown on the left relies on a sample of 10 airline firms, with an average revenue of USD 2.48bn. The average limits purchased is USD 13.7m.

There are no set rules to determine how much insurance limit is the correct amount to purchase as risk appetite does vary. We can also use the Probable Maximum Loss study (as provided by Cyber Advisory) & Cyber Self Assessment outcome to aid in supporting how much limits to purchase moving forward.

Case Study

05

MARSH

Data Breach Case Study

Hospitality

Incident

Swanbeach International disclosed a massive data breach affecting its *'Starstud guest reservation'* database as a result of a **faulty update**. The breach had actually begun in 2014 but was only discovered in September 2018. Hackers gained unauthorized access to the reservation system due to the vulnerability caused by the update, compromising the personal information of approximately **383 million** guests worldwide, including:

- Names
- Mailing Addresses
- Phone numbers/emails
- Passport numbers
- Arrival/Departure dates
- Payment card numbers and expiration dates
- This put guests at risk of identity theft, fraud and theft,

Legal Consequences and Third-Party Action

- Swanbeach faced numerous lawsuits from affected guests and regulatory investigations globally.
- The UK Information Commissioner's Office (ICO) fined Swanbeach GBP 18.4 million in 2020 for failing to protect customer data adequately under GDPR regulations.
- Class-action lawsuits were filed in the United States and other jurisdictions, seeking damages for negligence and failure to safeguard personal data.
- Swanbeach agreed to settlements, including compensation funds for affected customers and commitments to improve cybersecurity measures.
- The breach also led to increased scrutiny from regulators and heightened expectations for data protection in the hospitality sector.
- Customers no longer wanted to stay at Swanbeach as they were afraid that all of their data would be at risk

Recovery/Response powered by Cyber Insurance

The victim organization can submit costs incurred in relation to the previous section, but not limited to:

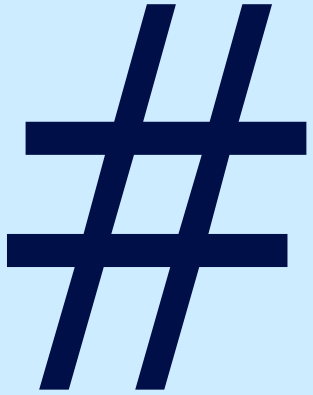
- Business interruption losses; lost revenue from disrupted hotel operations and increased operational costs.

Access to vendors to perform the following and related costs:

- Designing and implementing communication strategies
- Data and IT System restoration
- Notification of affected guests and regulatory authorities
- Monitoring costs to prevent misuse of leaked data
- **Liabilities; damages and defense costs arising from lawsuits and regulatory investigations/fines**
- Regulatory fines following a regulatory investigation
- Access to out-of-band communication platforms and crisis management resources to coordinate incident response

MARSH

Appendix A: Who are We



Marsh MENA Cyber Credentials

1. 9 experienced, in-region, Cyber Insurance Specialists
2. Market-leading Cyber insurance wordings
3. Facility and Captive Solutions
4. Round-tables, risk seminars, thought leadership
5. Access to DIFC, London and Singapore reinsurance markets
6. Close collaboration with Marsh Cyber Advisory teams

Simon Bell
Cyber Practice Leader
IMEA

Lewis Bennett
Cyber Broker
MENA

Zaina Oughli
Cyber Broker
MENA

Gulistan Yesilmen
Cyber Broker
MENA

Gregory Le Henand
Cyber Practice Leader
UAE

Angus Edwards
Cyber Growth Leader
MENA

Mariam Alriyami
Cyber Analyst
MENA

Abdulmohsin Aljalal
Cyber Growth Leader
KSA

Jodie Davies
Cyber Broker
MENA

• 72 hours

Marsh CyberWall wording

Bespoke and tested wording agreed by all insurers we work structured for clients

>$4 billion

in **premiums** placed globally; real time monitoring of market trends

25+

Years experience and Cyber Event data; pioneering innovative solutions and continuous servicing

#1 Leading broker in MENA

with over 50% market share in cyber insurance

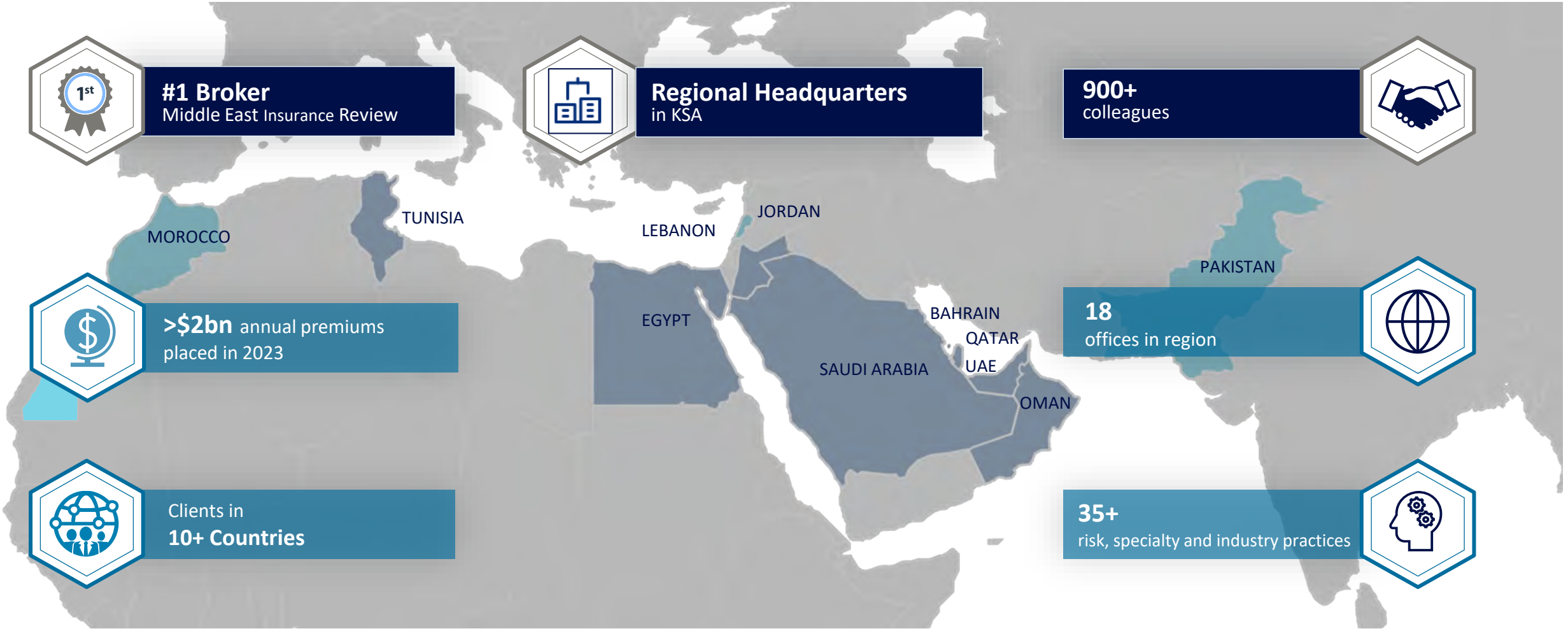
10,000+

Cyber Risk Self-Assessments on record ; driving broad view of risk scores and insurability drivers

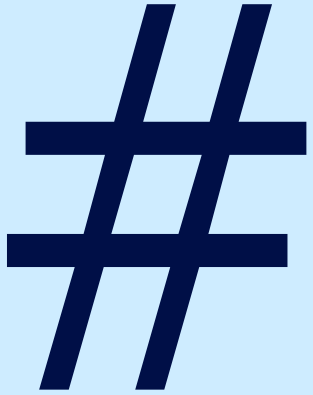
• 72 hours

MARSH

Marsh Regional Overview



Appendix B: State of the Market



State of Cyber Insurance Markets

Middle East and North Africa

Q1 2026 Review

Rates

Increased capacity-driven competition continues across MENA, where a large number of first-time buyers remain active.

Rate change in MENA markets in Q1 showed a more pronounced year-on-year decline than in the previous quarter, indicating an acceleration of market softening driven by increased capacity and competition.

Most renewal clients in the large corporate segment continue to leverage rate reductions by purchasing higher limits.

Coverage

Available Cyber Non-PD insurance capacity in the MENA region has exceeded 150M$ based on industry.

Cyber PD capacity can be written up to 450M$ depending on the industry. Insurers based in MENA region are investing in developing Cyber PD with theoretical capacity reaching to 65M$ where there is no aggregation with large consortiums.

Limit purchasing decisions are being heavily influenced by the risk quantification exercises.

Limits

With continued pricing pressure, carriers are focusing on product differentiation through broader and more bespoke cyber endorsements, and several market players are developing industry-specific wording.

Insurers are also increasingly embedding or partnering to provide risk-prevention and incident-response services alongside capacity.

Underwriters are placing greater emphasis on operational controls such as out-of-band communications when assessing terms, and demonstrated OOB controls can influence pricing and placement options

Threat Activity

Ransomware continues to hit retail, financial institutions and aviation, with attackers using sophisticated social engineering and layered extortion; recent Q1 incidents disrupted airport operations and affected airline partners.

Supply-chain compromises and rapid exploitation of newly disclosed vulnerabilities have caused prolonged manufacturing and service outages, increasing risk to OT environments.

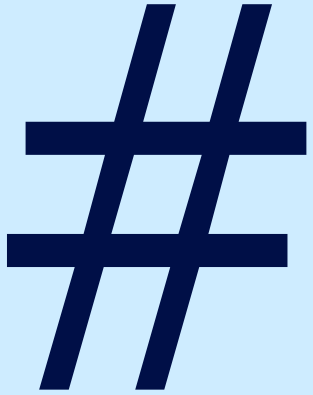
Widespread cloud-service interruptions further amplify systemic exposure, so resilience, rapid detection and tested response plans remain essential.

Q1 2026 saw a rapid uptick in cyber insurance buyers across MENA, driven by rising incident frequency and the rollout of local privacy laws. Pricing continues to soften, but the pace of rate reduction is moderating as market floors emerge. Ransomware remains the dominant threat and is evolving with more sophisticated social engineering and AI-assisted techniques, while supply-chain and cloud service events increase systemic exposure. Out-of-band communications and dedicated incident-management platforms have seen widespread adoption among multinationals and are proving critical to secure, coordinated response. Carriers are responding by broadening and differentiating coverages and by packaging prevention and response services, supported by healthy capacity and strong competition.

Sources: PDI Cyber Threat Landscape Report Q1 2026; AIR IT Group Quarterly Threat Report Q1 2026; GuidePoint GRIT 2026 Ransomware and Cyber Threat Report; Fidelis Security Q1 2026 trends; industry threat summaries from IBM X-Force and CrowdStrike Q1 2026 reporting.

MARSH

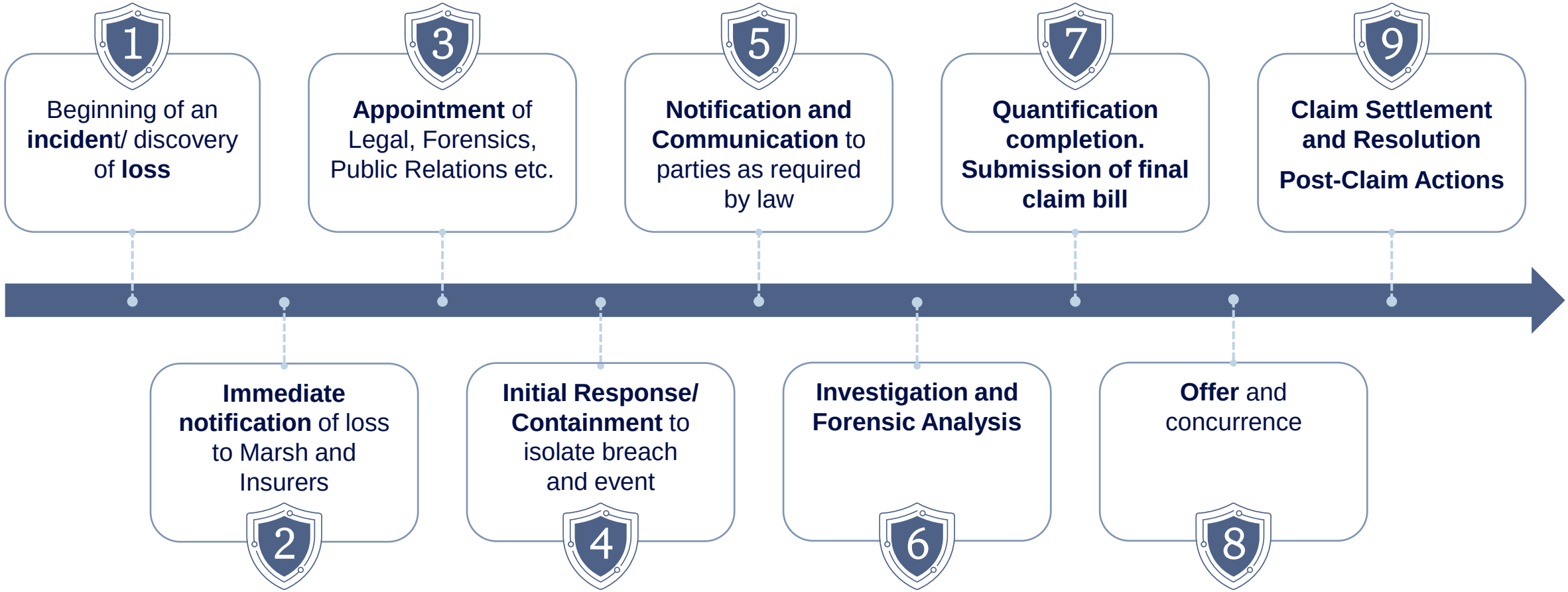
Appendix C: Claims Process



Insurance Claims Process

An Overview

Marsh have an established claims process to render rapid and efficient settlement and payment of claims, service and assistance in finalising claims to your benefit. A snapshot of the claims process is as follows:



For each of these steps, Marsh will be able to advise you of the best practices, the “Dos and the Don’ts” and assist with the collation of the required supporting documents to lead to the most favourable settlement outcomes.

MARSH

We are leaders in risk, strategy and people. One company, with four global businesses, united by a shared purpose to build the confidence to thrive through the power of perspective.