Assessing the potential financial impact of a cyber-attack is a challenge for many organizations. Cyber threats are pervasive and dynamic, and many businesses’ technology assets and dependencies are continually evolving.

Many organizations assess their cyber risk exposures qualitatively, using “traffic light” dashboards, descriptions, or relative rankings. But generalized, qualitative cyber risk assessments don’t yield meaningful insight into the potential financial cost of cyber events or guidance for decisions about investment in risk mitigation and transfer.

**QUANTIFICATION YIELDS BETTER DECISION-MAKING**

The fact is that cyber risk is an enterprise issue, not just a technical one. Cyber threats — like all major risks — must now be measured, expressed, and understood by a broad range of organizational stakeholders using economic quantification, the common language of business. Regulators, too, are requiring risk-based assessments that compel organizations to grapple with the financial size of their cyber exposures while addressing other enterprise threats.

Economic quantification places cyber risk within an organization's overall risk framework, and shifts the conversation from a technical discussion about threat vectors and system vulnerabilities to one focused on maximizing the return on an organization's cyber spending and reducing its total cost of risk.

**Most organizations that have a means to express their cyber risk do so qualitatively.**

**SOURCE: MARSH-MICROSOFT CYBER PERCEPTION SURVEY**

*How does your organization measure or express its cyber risk exposure?*

- We have no method to measure or express cyber risk: 34%
- Economic quantification, based on estimated financial losses within a timeframe, such as value-at-risk modeling: 11%
- Numerical scores or rankings within a fixed framework: 9%
- Descriptively, without using categories, numbers, or rankings: 14%
- Using categories such as “high/medium/low” or capability models such as “maturity levels” to benchmark against other organizations: 26%
- Implementation tiers within the NIST cybersecurity framework: 6%

**MARSH HELPS YOU QUANTIFY AND MANAGE CYBER RISK**

Marsh’s customized cyber risk assessment tools are purpose-built to help organizations understand and quantify their cyber risk exposure, and make smart decisions about their cyber risk mitigation and transfer strategies.
MARSH’S CUSTOMIZED CYBER RISK ASSESSMENTS AND ANALYTICS

Marsh has developed market-leading, proprietary analytic and modeling tools to help you accurately identify and quantify your cyber assets at risk, calculate the financial impact of a cyber-attack, and choose the right risk mitigation and transfer solutions. We offer a full suite of analytic options that can be tailored to your organization’s specific needs, budget, and data universe.

MEASURING THREATS

**CYBER THREAT ENVIRONMENT ASSESSMENT:** We apply big data insights on threat actor behavior and perception to evaluate the likelihood and intensity with which your organization might be attacked — and benchmark that risk against your peers.

**THIRD-PARTY CYBER RISK MONITORING:** We evaluate the cyber risk inherited from vendors that you do business with — then prioritize risk mitigation measures, such as heightened surveillance or contractual insurance obligations.

UNDERSTANDING VULNERABILITIES

**CYBERSECURITY PROGRAM MATURITY ASSESSMENT:** Our proprietary self-assessment questionnaire applies NIST-aligned security functions to rate the maturity of your cybersecurity program, including identifying areas of strength and flagging areas for improvement. The assessment helps you develop messaging to proactively address underwriter concerns, and is accepted by major carriers as a submission for cyber insurance.

**EU GDPR SELF-ASSESSMENT:** Through our proprietary self-assessment questionnaire, we help you gauge and score organizational readiness and compliance with the GDPR regulation, which took effect in May 2018. We identify areas of strength or those needing increased focus along five categories, including governance, planning, implementation, training/testing/security, and third-party vendors.

**Marsh GDPR Self-Assessment Readiness Tier**

<table>
<thead>
<tr>
<th>Readiness Tier Description</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early / Initial Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Awareness / Compliance Underway</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Preparation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Sample Company GDPR Readiness Subcategory Tiers**

- Governance
- Policy & Planning
- GDPR Implementation
- Training & Testing
- Third-Party Vendor
ANALYZING IMPACT

We deploy proprietary, cutting-edge risk analytics and tailored modeling to help you project potential losses from a cyber event using a range of detail and depth:

BUSINESS INTERRUPTION IMPACT MODELING: We benchmark and model the range of losses from a severe operational or network disruption in two ways:

1. Benchmarking potential losses of your organization from a NotPetya-severity event against actual losses of impacted firms.

2. Modeling a range of business interruption losses from cyber events, using company-specific attributes, external data, and proprietary Marsh data.

CYBER SCENARIO MODELING: We develop highly customized cyber event scenarios to identify potential types of losses and quantify the associated financial impact for your organization. We apply that information to help you identify priorities for mitigation action and guide your risk transfer decision-making about insurance gaps, limits, and coverage.

DATA BREACH IMPACT MODELING: We project the range of liability claims arising from simulated breaches based on recent events and cost trends. We analyze the composition of total event costs based on a range of factors such as event severity, including first-party costs — credit monitoring, notification costs, forensics, and call center expenses — and third-party costs, such as payments to card networks and regulatory actions.
WANT BETTER DATA TO DRIVE IMPROVED CYBER RISK DECISIONS? TALK TO MARSH CYBER EXPERTS.

A quantified assessment and financial analysis of your organization’s cyber risk exposure is an essential foundation for effective cyber risk management. Marsh’s proprietary cyber risk analytics and modeling services provide critical insight to help you better understand your specific organizational cyber exposures and directly inform your cyber risk investments, including insurance coverages, limits, and mitigation activities. After all, you can’t manage what you can’t measure.

To benefit from our cyber risk expertise and analytics leadership, contact your Marsh representative or:

THOMAS REAGAN
Cyber Practice Leader
+1 212 345 9452
thomas.reagan@marsh.com

THOMAS FUHRMAN
Managing Director, Cybersecurity Consulting and Advisory Services
+1 202 263 7827
thomas.fuhrman@marsh.com

Marsh’s Cyber Insurance Practice by the Numbers

80+ DEDICATED CYBER COLLEAGUES, AMONG MORE THAN 300 FINPRO COLLEAGUES.

PLACING MORE THAN $750 MILLION PREMIUMS ANNUALLY.

PIONEER OF 30 YEAR-OLD CYBER INSURANCE MARKET.

MORE THAN 6,000 CYBER AND E&O CLIENTS.