

# CYBER RISK ASSESSMENT SOLUTIONS



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%

#### QUANTITATIVELY

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%

#### QUALITATIVELY

Using categories such as “high/medium/low” or capability models such as “maturity levels” to benchmark against other organizations

26%

Descriptively, without using categories, numbers, or rankings

14%

Implementation tiers within the NIST cybersecurity framework

6%

## MARSH HELPS YOU QUANTIFY AND MANAGE CYBER RISK

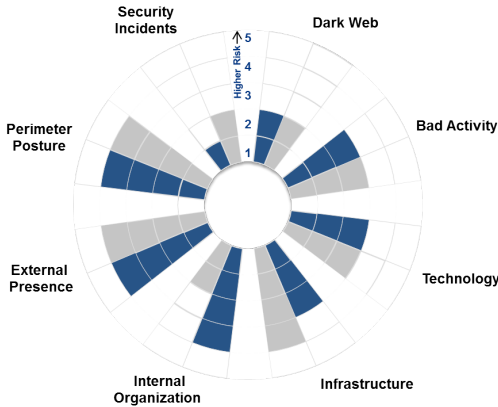
Marsh’s customized cyber risk assessment tools are purpose-built to help organizations understand and quantify their cyber risk exposure, and make smart decisions about their cyber risk mitigation and transfer strategies.

# MARSH'S CUSTOMIZED CYBER RISK ASSESSMENTS AND ANALYTICS

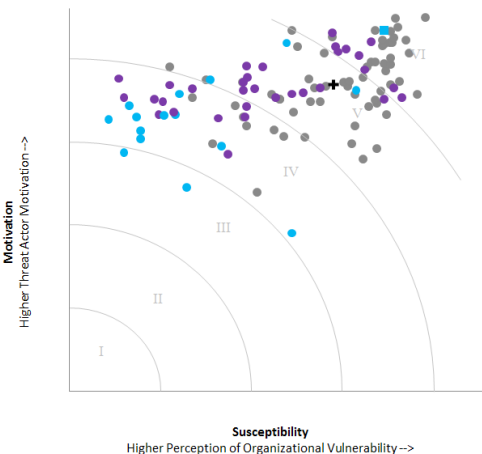
Marsh has developed market-leading, proprietary analytic and modeling tools to help you accurately identify and quantify your cyber assets at risk, calculate the financial impact of a cyber-attack, and choose the right risk mitigation and transfer solutions. We offer a full suite of analytic options 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.

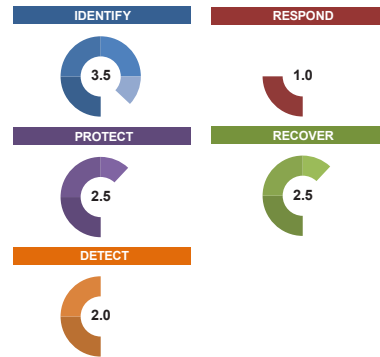


**THIRD-PARTY CYBER RISK MONITORING:** We evaluate the cyber risk inherited from vendors that you do business with — then prioritize risk mitigation measures, such as heightened surveillance or contractual insurance obligations.



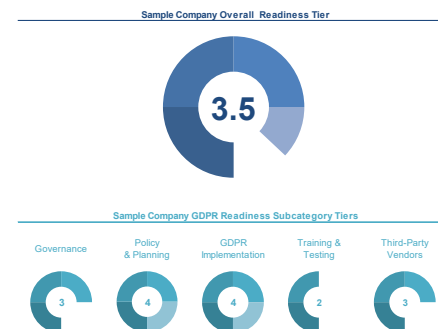
## UNDERSTANDING VULNERABILITIES

**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

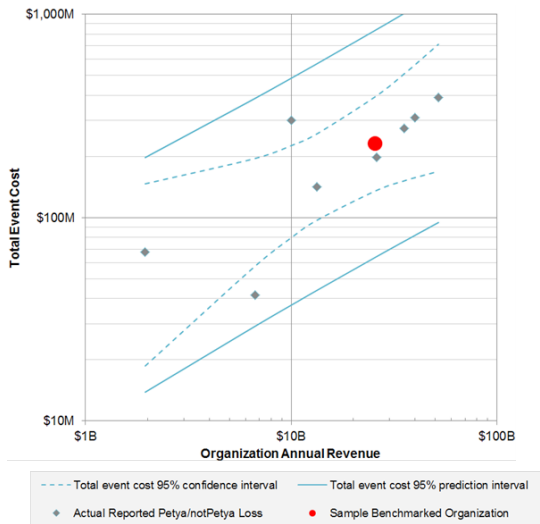


## ANALYZING IMPACT

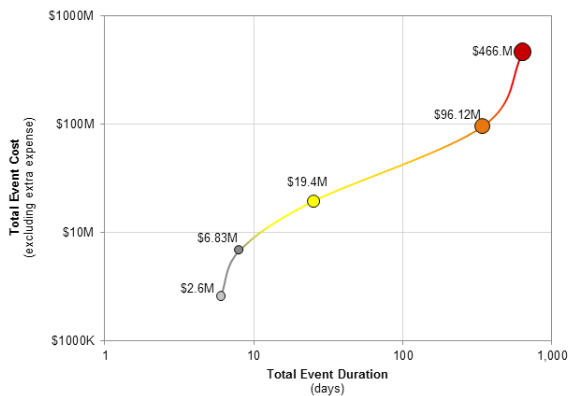
We deploy proprietary, cutting-edge risk analytics and tailored modeling to help you project potential losses from a cyber event using a range of detail and depth:

**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.



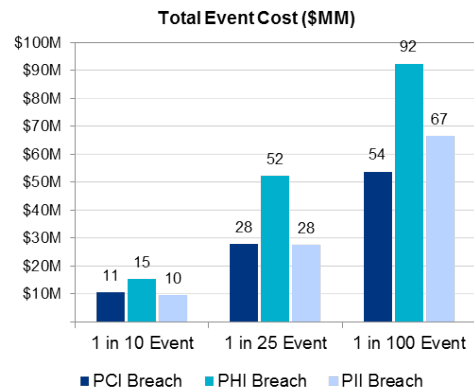
2. Modeling a range of business interruption losses from cyber events, using company-specific attributes, external data, and proprietary Marsh data.



**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.

EXAMPLE					
Executive Summary					
Company Name	Company Industry				
Sample Company	Manufacturing (NAICS 31-33)				
Scenario 1: Cyber Attack on Automation Systems Halts MMS Production					
Scenario Name	Cyber Attack on Automation Systems Halts MMS Production				
Event Class	CYBER ATTACK ON AVAILABILITY OF PRODUCTS OR SERVICES THAT THE COMPANY DELIVERS				
Event Element 1	Industrial Control System Compromise Causing Production Interruption				
Event Element 2	Industrial Control System Malware Affecting Quality Control				
Event Element 3	Damage/Destruction of Critical Physical System				
Cyber Event Summary					
Malware infected distributed control systems at the Samplesville plant, reprogramming devices and disrupting multiple processes in the production of advanced metal matrix composites. Production was suspended for 4.5 days. Additionally, two days of material was wasted and supply chain schedules caused two additional days before full production was achieved. Delivery delays affected downstream processes, ultimately delaying delivery of critical structural modules, and incurring financial penalties.					
Financial Impact Summary					
Gross Loss		Nominal Insurance Coverage		Net Loss	
Business Income Loss	Insurance analysis is based on the ACTUAL Acropolis program. Nominal Coverage does not consider limit or retention.				
Est. Lower Bound	Est. Upper Bound	Est. Lower Bound	Est. Upper Bound	Est. Lower Bound	Est. Upper Bound
\$573,000	\$1,404,000	\$573,000	\$1,404,000	\$0	\$0
Incident Response Costs					
\$49,000	\$68,000	\$49,000	\$68,000	\$0	\$0
Restoration Costs					
\$159,000	\$243,000	\$115,000	\$174,000	\$44,000	\$69,000
Litigation Costs					
\$979,000	\$1,065,000	\$0	\$0	\$979,000	\$1,065,000
Other Business Impact					
\$110,000	\$200,000	\$0	\$0	\$110,000	\$200,000

**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

 <b>80+</b> DEDICATED CYBER COLLEAGUES, AMONG MORE THAN 300 FINPRO COLLEAGUES.	PLACING MORE THAN <b>\$750 MILLION</b> PREMIUMS ANNUALLY.
 <b>PIONEER OF 30 YEAR-OLD</b> CYBER INSURANCE MARKET.	MORE THAN <b>6,000</b> CYBER AND E&O CLIENTS.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.