MARSH

Cybersecurity Consulting
and Advisory Services

CYBER EXPOSURE QUANTIFICATION (CYBERXQ)

Too often cyber risk analysis is conducted with simplistic estimation methods based on broad assumptions that are not specific or appropriate for a given company. While less expensive in the short term, these methods may not tell the full story and may leave your organization uninformed about its true exposure.

Marsh Risk Consulting's (MRC) cybersecurity experts are ready to collaborate with your team to use scenario analysis to estimate your cyber exposure using our purpose-built CyberXQ tool. With CyberXQ, we can efficiently define cyber event scenarios and estimate resulting losses using cost models tailored to specific impacts. We can then overlay that with an analysis of potential insurance coverage for loss of business income and multiple categories of extra expenses.

We work with you to systematically develop scenarios based on cyber threats to your industry and business model, recent events, special interest areas (e.g., regulatory expectations), and other factors. Our approach includes insurance analysis, as our consultants work closely with Marsh brokers to identify the coverage gaps and needs highlighted by the scenarios.

The scenarios and analyses can also illuminate opportunities for improvement in cyber risk management and resiliency such as business continuity planning, incident response, and stress testing.

SCENARIO STRUCTURE AND APPLICATION

Our CyberXQ scenarios are constructed using a strategic building block approach. The scenarios are classified and structured by:

- **Cyber Event Classes**: The top-level categories of cyber events such as availability events, confidentiality events, or others, applicable to your industry.
- **Cyber Event Elements**: Specific event components that can combine into compound cyber scenarios. Within each cyber event class, there can be many cyber event elements – just as in the real world.
- **Scenario Narrative**: A description of the hypothetical cyber event at your organization.

Who it's for

- Executives in risk, compliance, and IT Security who want a dollar estimate of their organization's cybersecurity risk exposure.

What you get

- Insight into the potential dollar impact of cyber-attacks on your business.
- An intuitive, scenario-based methodology with results that are traceable and understandable by executives.
- Custom cyber event scenarios designed specifically for your unique business to give you a more holistic understanding of your cyber risk.
- Guidance for optimizing cyber risk management investments.
- Results that enable your cyber insurance brokers to better analyze coverage gaps and limits and make custom cyber insurance recommendations.

EXAMPLE

Executive Summary

Company Name	*Company Industry*
Acmeprimo International	**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 East Anodyne 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 Acmeprimo 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

Two to six CyberXQ scenarios are usually needed to characterize your exposure. Factors affecting the number of scenarios include complexity of your business model, its dependence on information technology, and the overall cyber "attack surface."

After working with you to define scenarios, Marsh experts will work with your team to gather specific scenario information and then analyze the scenario-specific business impacts, such as loss of business income, incident response costs, system and data restoration costs, extortion, fines, and litigation costs, brand image restoration, and other costs that may be related to the cyber event.

INFORMING YOUR CYBER INSURANCE DECISIONS

CyberXQ provides you with a complete and concise report that documents the cyber event scenario, key assumptions, and impact in dollar terms. Included in the report is analysis by Marsh cyber insurance advisors, which identifies how your current or prospective insurance program would respond to the scenario events. Your Marsh broker can then advise you on optimizing your insurance program in terms of coverage, policy language, limits, and retention.

To learn more about how these services and our full range of cybersecurity consulting and advisory capabilities can help you understand your cyber risk exposures, manage your cyber risks, and protect your business from cyber-attacks, please visit www.marshriskconsulting.com, contact your local Marsh representative or:

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