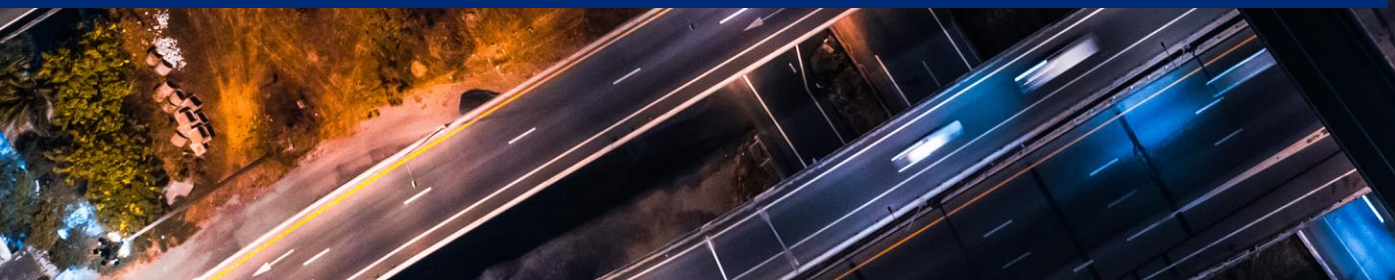
Marsh

The Road to Resiliency Webinar

June 17, 2021



Webinar Agenda

Welcome & Introductions – Lisa Kremer, SVP, Marsh Strategic Risk Consulting Practice Leader

Business Resiliency Landscape & Pain Points

- **ERM (risk identification and quantification)** – Andrew Tait, Marsh Specialty Advisory - Strategic Risk Practice Lead
- **Pandemic Planning / BCP / Crisis Management** – Renata Elias, Marsh Advisory – Crisis/Incident Management Lead
- **Digital Supply Chain / Cyber (ransomware)** – Jim Holtzclaw, Marsh Advisory - Cybersecurity Consulting

Q&A – Lisa Kremer SVP, Marsh Strategic Risk Consulting Practice Leader

Industry Remarks

- **Retail Wholesale Food and Beverage –** Mac Nadel, Marsh Retail/Wholesale, Food & Beverage Industry Leader
- **Manufacturing & Automotive** – David Carlson, Marsh US Automotive & Manufacturing Industry Practice Leader

Thank You and Close – Lisa Kremer SVP, Marsh Strategic Risk Consulting Practice Leader

Today’s speakers

Lisa Kremer, SVP
Marsh Advisory
Strategic Risk Consulting Practice Leader
Lisa.S.Kremer@marsh.com

Mac Nadel, Practice Leader
Marsh
National Retail/Wholesale, Food & Beverage Industry
mac.d.nadel@ocs.mmc.com

David Carlson, Practice Leader
Marsh
U.S. Manufacturing & Automotive Industry
David.T.Carlson@marsh.com

James Holtzclaw, SVP
Marsh Advisory
Cybersecurity Consulting & Advisory Services
James.Holtzclaw@marsh.com

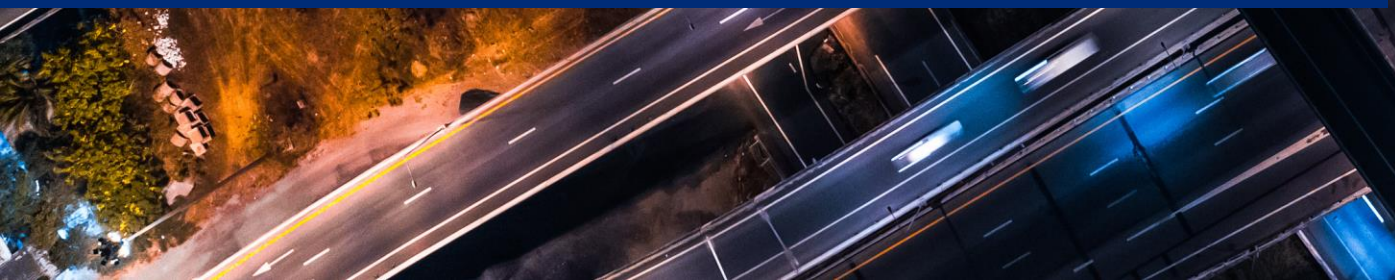
Andrew Tait, Managing Director
Marsh Specialty Advisory
Lead Consultant
Andrew.Tait@Marsh.com

Renata Elias, SVP
Marsh Advisory
Lead Consultant
Renata.Elias@marsh.com

Marsh

ERM (Risk Identification and Quantification)

Andrew Tait, Managing Director
Marsh Specialty Advisory
Lead Consultant



Enterprise Risk Management

Risk Identification and Quantification……and Treatment and Financing

To manage risk you need to

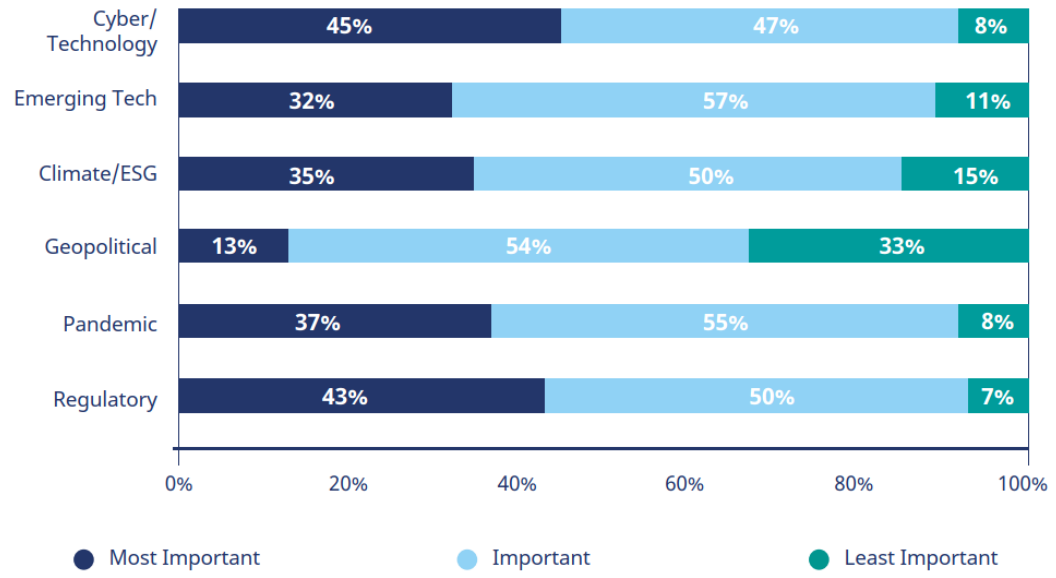
- Identify it
- Understand it
- Quantify it (*So what if it happens*)
- Assess how well it is controlled
- Prioritize it
- Manage it (*To reduce likelihood or severity*)
- Finance the risk that remains

- Across a range of risks categories

From traditional OPERATIONAL and STRATEGIC Risks

- To an ever-changing set of Emerging Risks…

01| **There is broad agreement on the importance of various emerging risks.**



Source: *Marsh Risk Resilience Report_FINAL_May 2021*

Under the ERM umbrella

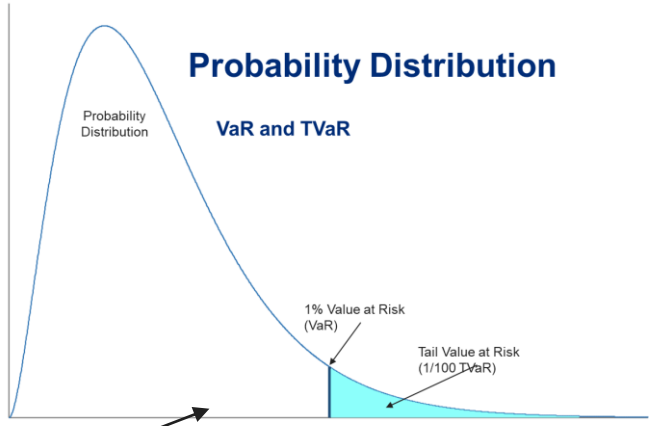
Tools/Techniques to consider

- Data Collection and Mining – Visualization
- Leverage your smart people
- Identify critical value drivers
  - And what can impact them…
- Regular review of risks with Cross Functional team
  - Risk Council can play this role
- Build accountability mechanism(s)
- Audit current ERM risk identification and triage processes - do they support cross functional action
  - Does it help executive management?
  - It is timely?

Data/Analytics → Risk Financing

To drive and support decision making

- Deploy more timely and robust modelling/visualization tools to support issue identification and decision making
- Include input from the experts – from your firm and outside experts (Marsh)
- Model different outcomes across different likelihoods – don't get surprised by the tail
- Model different mitigations to optimize decision making
- Design external risk financing to cover extreme events that can't be managed away
  — using balance sheet and captives to fund foreseeable/expected losses + market



	Per Occurence Limit	Aggregate Sub-Limit	Retention	Average Cost (M)	1-in-100 TVaR (M)
Program 1 (Lower Limit)	250M (CS, WS) 143M (QKE, FLD) 25M (Fire)	250M (CS, WS, Fire) 143M (QKE, FLD)	15M Per Occ. 30M Agg.	$17.37	$565.83
Program 2 (Current)	500M (CS, WS) 285M (QKE, FLD) 50M (Fire)	500M (CS, WS, Fire) 285M (QKE, FLD)	15M Per Occ. 30M Agg.	$18.93	$494.66
Program 3 (Higher Limit)	750M (CS, WS) 428M (QKE, FLD) 75M (Fire)	750M (CS, WS, Fire) 428M (QKE, FLD)	15M Per Occ. 30M Agg.	$19.10	$452.05
Program 4 (Higher Limit)	1B (CS, WS) 570M (QKE, FLD) 100M (Fire)	1B (CS, WS, Fire) 570M (QKE, FLD)	15M Per Occ. 30M Agg.	$19.14	$423.73
Program 5 (Lower Retention)	500M (CS, WS) 285M (QKE, FLD) 50M (Fire)	500M (CS, WS, Fire) 285M (QKE, FLD)	7.5M Per Occ. 22.5M Agg.	$21.34	$499.81
Program 6 (Higher Retention)	500M (CS, WS) 285M (QKE, FLD) 50M (Fire)	500M (CS, WS, Fire) 285M (QKE, FLD)	22.5M Per Occ. 45M Agg.	$17.81	$494.16
Program 7 (Higher Limit/Retention)	1B (CS, WS) 570M (QKE, FLD) 100M (Fire)	1B (CS, WS, Fire) 570BM (QKE, FLD)	22.5M Per Occ. 45M Agg.	$18.03	$424.41

Case Study

Enterprise Risk Management

Client situation

- Globally integrated retail manufacturer of convenience store products.
- Executives recognized a customer fulfillment exposure due to a large range of global manufacturing and distribution risks.

Approach

- Marsh and client SMEs integrated current processes and system risk knowledge to develop a critical supplier and owned supply chain risk view that was agnostic to cause of risk.
- Characterized and modeled by risk category, geography, or exposure type.
- Approach focused on building a management decision making process.

Results

- New process with integrated visualization tools that allows business to easily identify bottlenecks or particular risk matters and report to executive management in a timely manner.
- Increased speed of support for resiliency and helps to create a more nimble risk management function.

Marsh

Pandemic Planning / BCP / Crisis Management

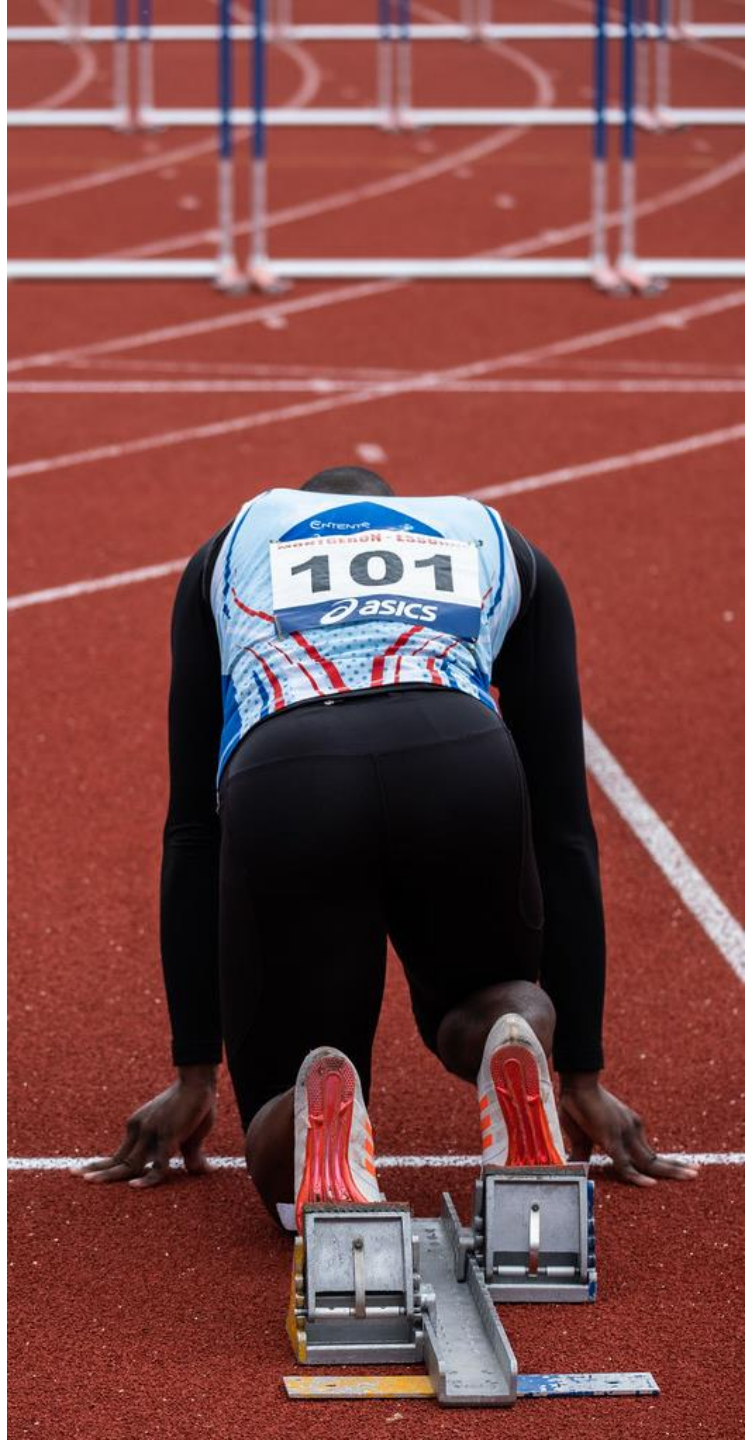
Renata Elias, SVP
Marsh Advisory
Lead Consultant

Crisis Management

It is not if, but when…

A crisis can be a **defining moment** for an organization, either **severely threatening** or **greatly enhancing** its people, operations, customer loyalty, community standing, financial performance, and reputation.

- An overall response structure/framework.
- Process for getting out of the ‘starting blocks’.
- Understanding the importance of staying in your own ‘lane’.



The Road to a Crisis Response Capability

Four step approach

Assemble and Formalize

STEP 1

- Project plan and timeline
- Project team
- Overall response/ governance structure and policy guidance documents

Review, Update, and Develop

STEP 2

- Update current plans to align with overall response and governance structure
- Outstanding plans
- Plan update schedule

Training and Exercising

STEP 3

- Overall training/ exercise program
- Team training
- Employee awareness
- Team exercises

Integration

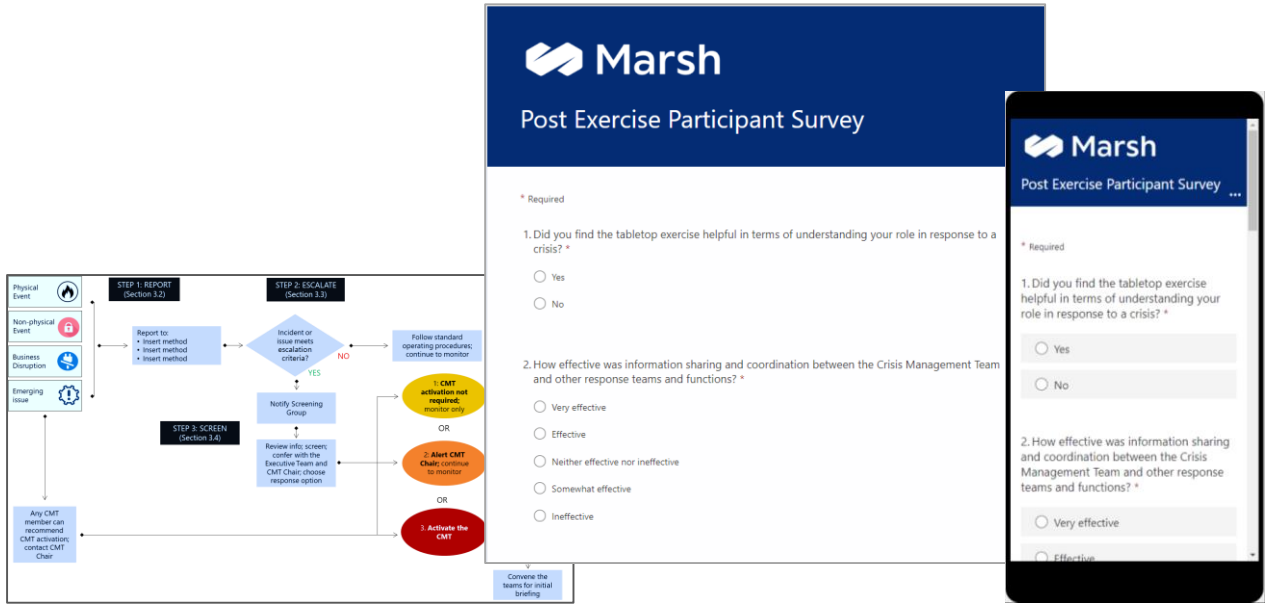
STEP 4

- Joint exercises
- Identify gaps, areas of improvement
- Action plan and process to implement solutions

How Marsh can help

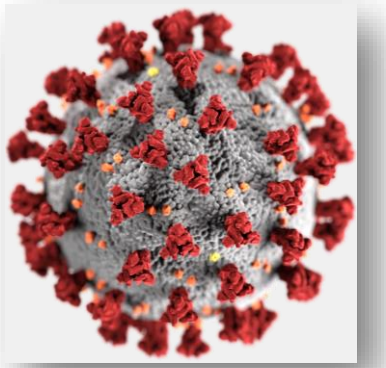
Over 30 years of experience

- Gap assessment – ‘silos or an umbrella’.
- Crisis management planning – ‘a crisis is not business as usual’.
- Tabletop exercises – building ‘muscle memory’.



Case Study

COVID highlighted the need



Client situation

- Leading manufacturer with global operations and manufacturing footprint.
- Executive Team recognized a need.
- Identified the need for a structured Corporate response to the COVID outbreak and its impact on people and operations.

Approach

- Collaborated with the corporate planning team.
- Facilitated on-site planning sessions.
- Developed a crisis management framework.
- Reviewed and updated the corporate pandemic plan.

Key Results

- Reviewed plans and procedures.
- Provided advisory recommendations and support services through facilitated planning sessions.
- Tailored the framework and plan to the client and its operations and culture.
- Ensured alignment and integration across and up and down the organization.

Marsh

Digital Supply Chain / Cyber (ransomware)

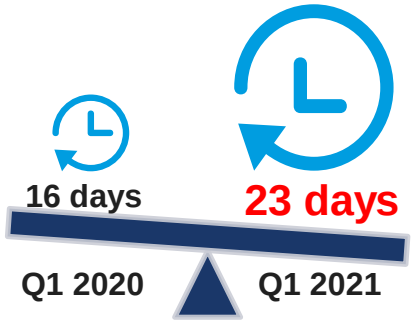
James Holtzclaw, SVP
Marsh Advisory
Cybersecurity Consulting & Advisory Services

Cyber Trends

Dominated by Ransomware, regulations & supply chain cyber risk

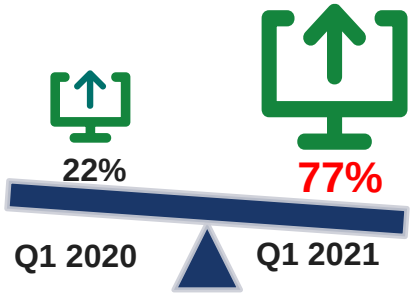
Ransomware attacks continue to increase in frequency, severity & sophistication:

Average downtime:



44% YOY increase

Cases with data exfiltration:



250% YOY increase

$ **~$800K** average ransom payment;
$40M highest ransom paid to date

Reduction in average ransom payment is attributed to lack of confidence that data is being deleted, and as a result fewer companies actually paid the demands in Q1 2021. The ability to restore from back-ups is key. However, overall costs and downtime are still on the rise and largest demands are $10M's+.

Privacy regulations are intensifying and there's still a patchwork approach:

- **GDPR** fines are growing (~$27M BA, ~$24M Marriott, ~$41M H&M)
- **CCPA** (California Consumer Privacy Act) and similar legislation (i.e. VA CDPA) allow for private rights of action and require additional compliance efforts.
- **BIPA** (IL Biometric Information Privacy Act) litigation is expensive and is on the rise with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions.

Supply chain and systemic risk now garner more focus:

- **Aggregation** exposure a concern for underwriters
- **Systemic loss** – possible cyber risks:
  - Common vulnerabilities – in hardware or software
  - Common dependencies – vendors (such as cloud providers) and software
- **Cyber events** are driving increased scrutiny: SolarWinds, Accellion, & Microsoft Exchange

Sources: Coveware Ransomware Blog & Baker Hostetler 2021 DSIR Report

Cyber Incident Management

Cyber Incidents are crises that must be managed efficiently and effectively by the organization to minimize the impact both financially and for the organization's reputation…

- Ransomware is a significant and growing risk for organizations requiring proactively planning.
- Includes understanding cybersecurity risks associated with Third Party Vendors who have authorized access to the organization's data and IT systems.
- Organizations must have the following to minimize Ransomware impacts:
  - ✓ Sound, encrypted, and offline current backups for critical data and applications. These backups must be tested frequently for effective restoration when required.
  - ✓ In addition to a Backup System, effective Cybersecurity Controls including the following are necessary to minimize Ransomware impact:
    - MFA/2FA for Enhanced Access Control
    - A Phishing Aware and Trained Workforce
    - Monitoring of Critical Data & Applications
    - Logged and Monitored Networks
    - Secured Endpoints
    - Hardened Configurations

Cyber Incident Response Planning and Tabletop Exercises

An effective Cyber Incident Response Plan is critical in being able to effectively and efficiently respond to a Ransomware or Cyber Incident when it occurs. Practicing with the CIR Team and Senior Leadership is key to developing "Muscle Memory" in CIR decision making…

Marsh CIR Plan Development Approach

1 Discover

- Cyber Incident Response (CIR) Plan Strategy, Objectives and Goals (consistent with NIST SP 800-61: *Computer Security Incident Handling Guide*)
- Identify stakeholders, CIR Team members and responsibilities
- Document CIR Team activation process and Team Contact Info
- Document all information and develop the CIR Plan Outline

2 Develop & Refine

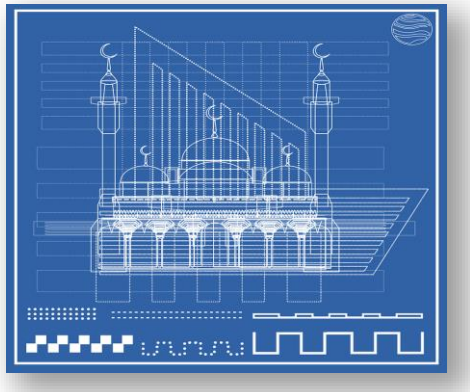
- Develop Draft CIR Plan implementation detail
- Document detailed processes, activities, and templates; refine the plan
- Develop incident information escalation procedures
- Identify and formalize CIR external partner support
- Conduct CIBR event "Dry Run" with CIR Team

3 Test & Finalize

- Plan and Conduct CIR Tabletop Exercise and document results
- Update/refine final CIR Plan and processes based on final inputs and exercise results
- Recommend a periodic Cyber Tabletop Exercise timeline with improvement goals
- Establish CIR Plan annual review process

Cyber Case Study

The Pandemic has increased the need for Cyber Incident Response (CIR) preparedness…



Client situation

- Client is a leading construction firm with international operations across North America.
- Key members of the Executive Team recognized the need to have a formalized Cyber Incident Response (CIR) Plan that would support effective and timely cyber incident response.
- Plan addresses Ransomware.

Approach

- Marsh reviewed Client's existing cyber policies and procedures, including informal processes.
- Marsh identified a model for the Client's CIR Plan and initiated work on developing tailored plan.
- Marsh developed supporting information to guide and assist the Client in responding to a Cyber Incident.

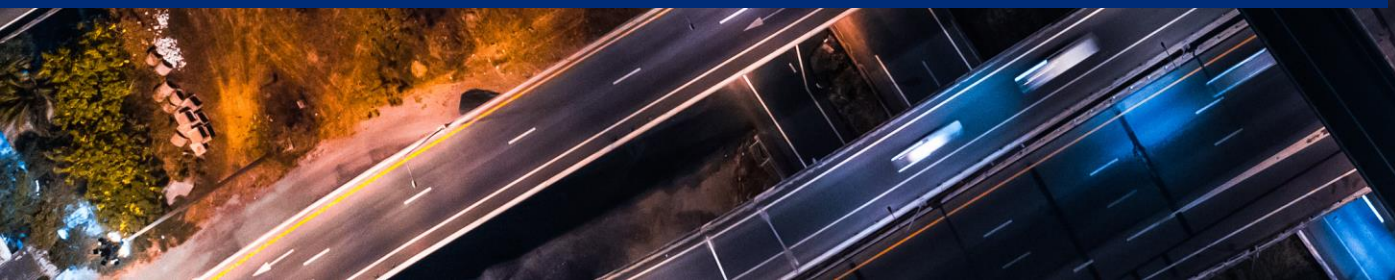
Delivery

- Marsh worked closely with Client's cybersecurity leader in developing an outline and refining content for the plan.
- Gathered information to build a plan tailored to Client's unique objectives.
- Marsh held workshops to identify requirements and walk through how plan applies in responding to a significant cyber incident.
- Marsh conducted "Cyber Scenario Dry Run" to illustrate the value of plan content.

Marsh

Q&A

Lisa Kremer, SVP
Marsh Advisory
Strategic Risk Consulting Practice Leader



Marsh

Industry Remarks

Mac Nadel – Retail/Wholesale, Food & Beverage Leader
David Carlson – Manufacturing and Automotive Leader

Thank you for attending!

For more information on how Retail Wholesale Food and Beverage companies can become more resilient, visit our dedicated page.

For more information on how Manufacturing and Automotive companies can become more resilient, visit our dedicated page.

Or call your Marsh representative

A business of Marsh McLennan