MARSH

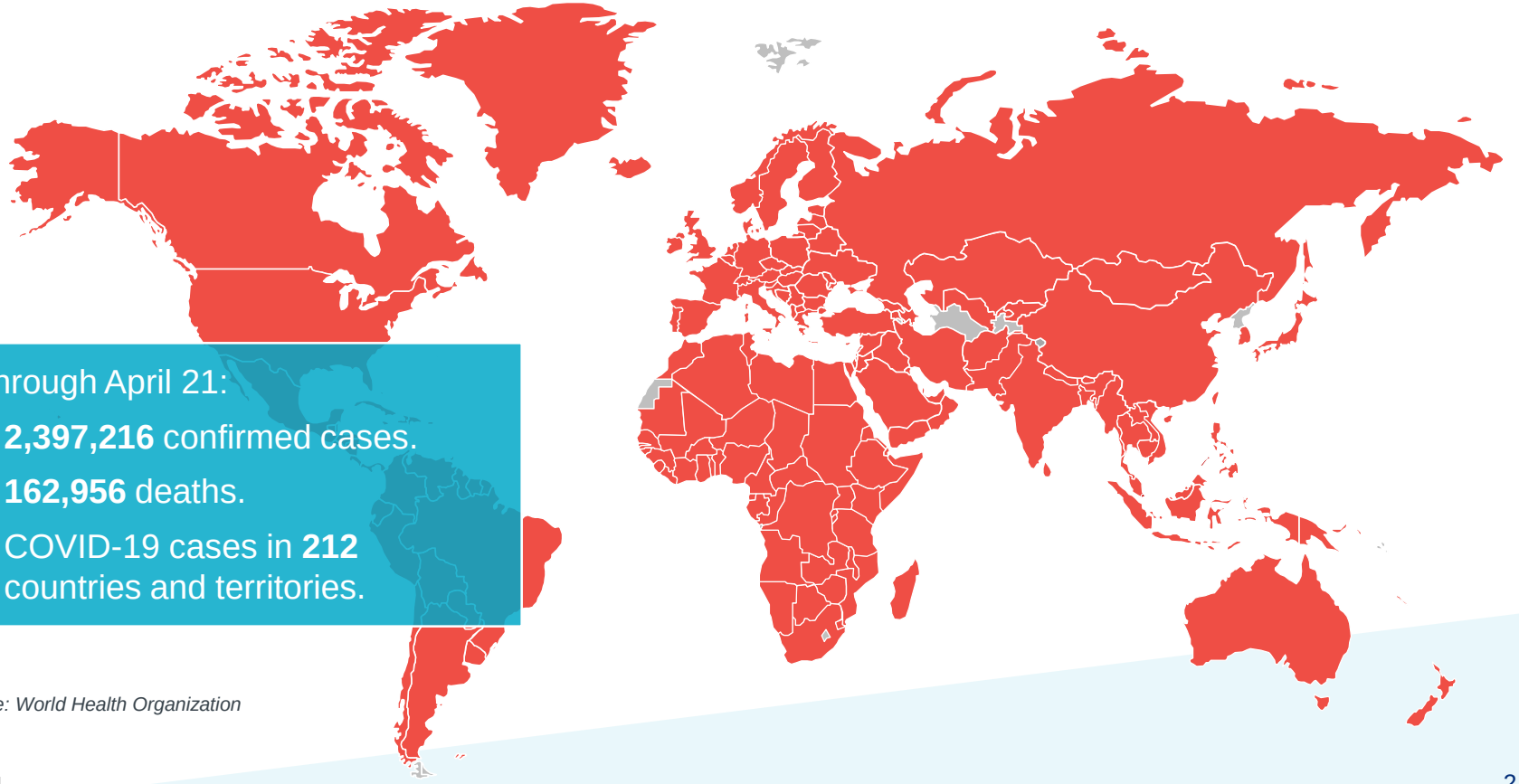
Managing Cyber and Supply Chain Risk During the Pandemic

April 22, 2020

MARSH & McLENNAN COMPANIES

Managing Cyber and Supply Chain Risk During the Pandemic

COVID-19 Continues to Spread Globally

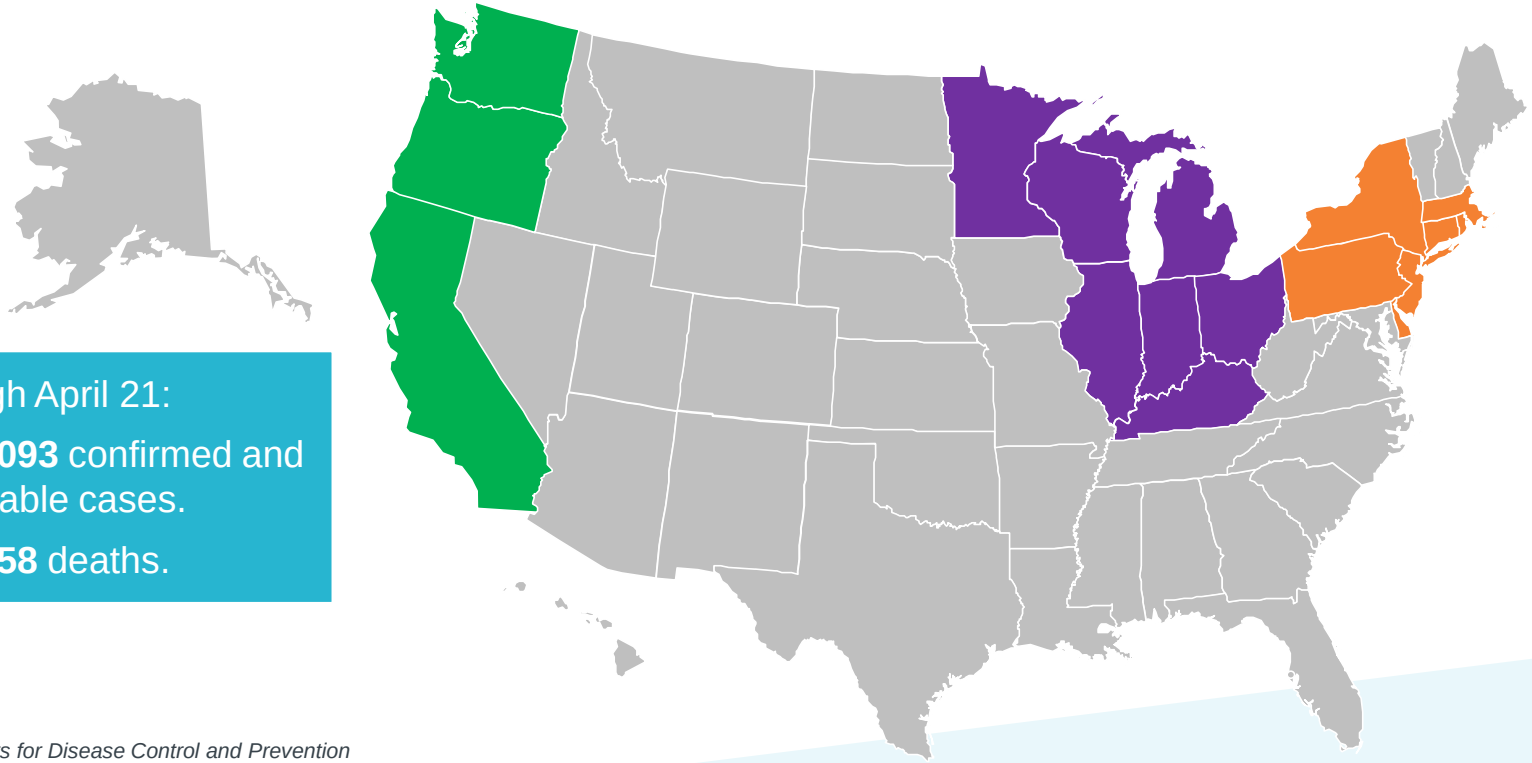


Through April 21:

- **2,397,216** confirmed cases.
- **162,956** deaths.
- COVID-19 cases in **212** countries and territories.

Source: World Health Organization

Managing Cyber and Supply Chain Risk During the Pandemic
States Coordinating Their Approaches



Through April 21:

- **776,093** confirmed and probable cases.
- **41,758** deaths.

Source: Centers for Disease Control and Prevention

Managing Cyber and Supply Chain Risk During the Pandemic
Global Supply Chain Challenges

- Global supply reduction of 20% to 80% amid pandemic.
  - Industries in China coming back online, but others still in or moving toward confinement.
  - Fluctuating demand:
    - -50% to -80% for aviation.
    - +30% for fruits and vegetables.
  - Production shutdowns common.
- Outlook:
  - Multiple waves.
  - Recovery? Six to 18 months.
  - Back to a ***new*** normal.

Managing Cyber and Supply Chain Risk During the Pandemic
What's Different About COVID-19?

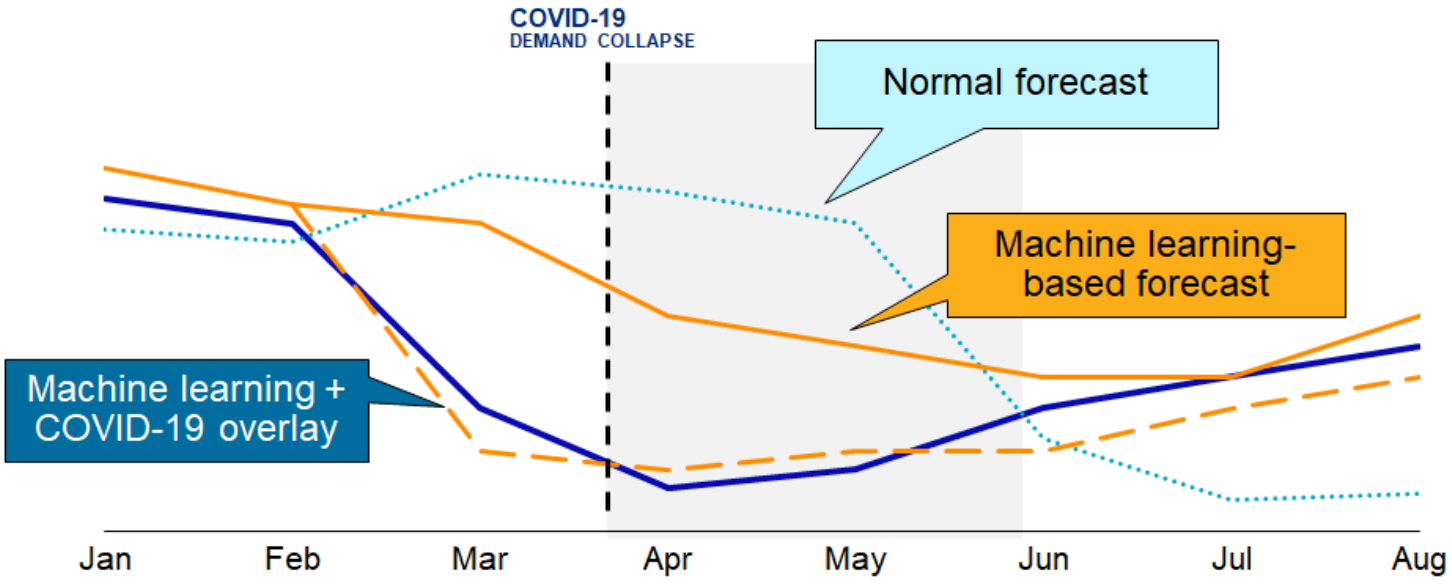
1. Time lag.
2. Globally dispersed solutions.
3. Demand – supply – operations – regulation.

What Businesses Can Do

- Short-term:
  - Focus.
  - Transparency.
  - Liquidity.
- Medium-term:
  - Scenario planning.
  - Bluebooks.
- Longer-term:
  - Shifts in value creation.
  - Risk management.

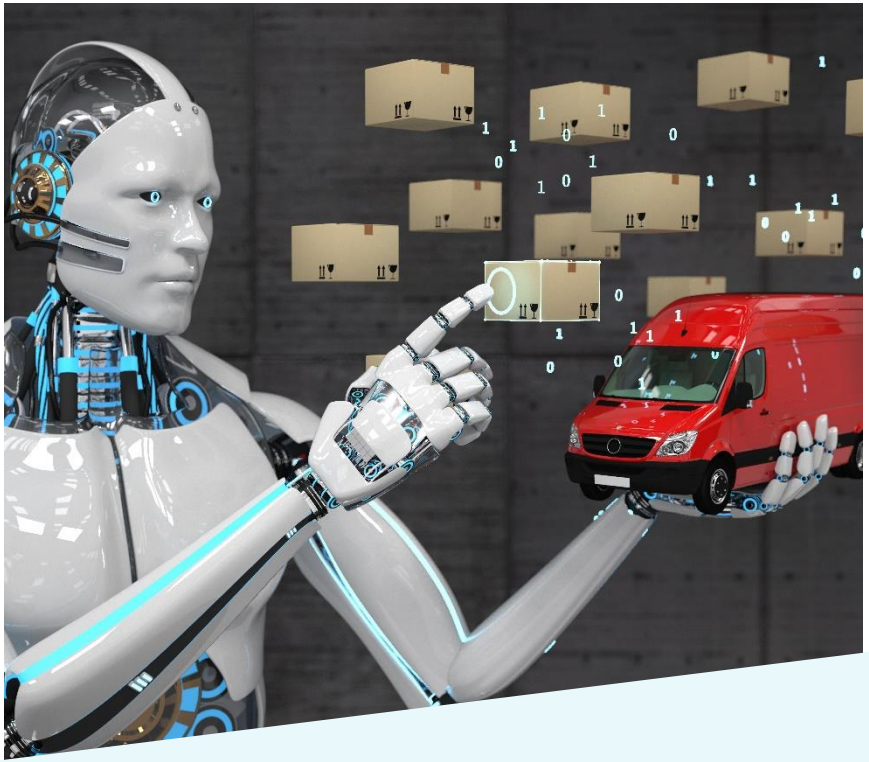
Managing Cyber and Supply Chain Risk During the Pandemic
Short-Term Priorities

- Focus.
- War room.
- Transparency.
- Agility.
- Liquidity.



Managing Cyber and Supply Chain Risk During the Pandemic
Medium- and Long-Term Planning

- Medium-term priorities:
  - Scenario planning.
  - Bluebook measures.
- Future risks and opportunities:
  - Shift in value pools and industry structures.
  - Digitalization.



Managing Cyber and Supply Chain Risk During the Pandemic
Cyber Threats Growing

- The pandemic could create more opportunities for cyber attackers.
  - Home networks are potentially less secure.
  - Privacy policies may be relaxed.
- Phishing and social engineering events are using the coronavirus and COVID-19 as hooks.
- Corporate technology systems are strained.
  - IT teams are addressing remote workforce problems.
  - Technology failures and business interruption are more likely given greater demands.

Managing Cyber and Supply Chain Risk During the Pandemic
How Cyber Insurance Policies Apply

Typical Coverages

- Breach/event response.
- Network business interruption.
- Ransomware event costs.
- Data recovery and restoration.
- Ransom event costs.
- Privacy liability.
- Reputational harm.
- Contingent business interruption.
- Privacy regulatory defense.
- Pre-breach loss prevention and mitigation.

Exclusions and Limitations

- Coverage excluded for failure of power, utility, mechanical, or telecommunications (including internet) infrastructure not under the insured's direct operational control.
- Coverage may only apply to voluntary shutdowns to prevent the spread of malware or limit damage.
- Computer system/network definitions may be limited.
- Policies may require:
  - Human or programming "error."
  - Proof of testing or patches.
  - Proof of system use prior to failure.

Managing Cyber and Supply Chain Risk During the Pandemic
Coverage and Renewal Recommendations

- Know what data and assets you have and where it is.
- Know your policy.
  - Review key language.
  - Understand how coverage, including incident response services, applies.
- Be ready for renewal discussions and scrutiny from underwriters about:
  - Business resilience.
  - Expanded attack surfaces.
  - How reliance on technology affects your response to disruptions.

Potential Questions from Underwriters

- How is COVID-19 affecting your operations?
- How are you managing access and device controls as employees work remotely?
- Is the pandemic affecting budget and resources for non-revenue generating departments?
- What's your ERM process? Can you share details about your BCP and disaster recovery programs?
- How has your supply chain been affected? What critical vendors are affected? Have you identified replacements?
- What liability management activities is your ERM team addressing?

Managing Cyber and Supply Chain Risk During the Pandemic
Cybersecurity Priorities

1

IT infrastructure

- Functions requiring secure environments.
- IT service provider dependencies.
- Secure access solutions.

2

Cyber operations

- Software updates.
- IT help desk capacity and hours.
- Analysis of alerts and audit logs.
- Multi-factor authentication.
- Reporting channels for employees.

3

Guidance for employees

- Phishing threats.
- Home and public Wi-Fi.
- Personal and family use of company equipment.
- Document management.

COVID-19’s Long-Term Economic Implications

Join Marsh again on **Wednesday, May 6**, at 11 a.m. EDT, for a closer look at what COVID-19 means for the US and global economies and more information and insights on how you can manage critical risks.

Visit marsh.com to register.

FEATURED SPEAKER

Sergio Rebelo, MUFG Bank Distinguished Professor of International Finance, Kellogg School of Management