The rise of operational losses from cyber attacks

Four steps to upgrading your BCM for Cyber Risk

Two in three companies have yet to upgrade their 'analogue' BCM strategies to meet the challenges of the new digital environment and increasing threat from ransomware attack.

Accelerated digital transformation and the adoption of 'Industrial Internet of Things' (IIoT) has exposed more business processes, OT assets, and supply chains to a variety of disruptive cyber events. As this transformative journey continues, it is now vital that financial exposures to disruptive cyber events are addressed as a priority within business continuity planning.

Emerging cyber threat

However, as organisations continue to invest in connecting more of their business to the web, not all companies have upgraded their legacy Business Continuity Management (BCM) plans and processes to mitigate the increased cyber threat - and the operational and reputational losses that could result.

Our research has identified that two in three companies have poorly defined strategies for disruptive cyber events in their legacy plans and more concerning, the majority of companies across the manufacturing, retail, transportation and construction industries have no plans to mitigate financial losses from disruptive cyber events.

Increase in ransomware claims

Threat Actors are upping their game and exploiting critical dependencies to digital technologies. Tracing the exponential trajectory of digital transformation investment, ransomware claims have increased by over 400% since 2018 and disruptive cyber events are contributing to 58% of insurer losses. These ransomware attacks are now resulting in losses that can exceed $100m.

+400%
increase in disruptive cyber events[1] in the form of ransomware that account for up to
58%
of insurer losses[2].

2 in 3
companies have inconsistent and informal approaches to Business Continuity Planning for disruptive Cyber events[3].

+51%
of companies in the manufacturing, retail, transportation, and construction industry have no BCPs to mitigate financial losses from disruptive Cyber events[4].

Statistics highlighted in this report have been extracted from Aon's proprietary analytics Cyber Quotient Evaluation (CyQu) platform 2020/2021.

[1] Aon Cyber Risk Consulting Research. 486% increase in ransomware events from Q1 2018 to Q4 2020.
[2] Aon Cyber Risk Consulting Research. Q1 2021 Underwriter Survey.
[3] Aon CyQu data
[4] Aon CyQu data

Evolving landscapes

As the threat landscape continues to evolve resulting in disruptive impacts to many businesses, insurance carriers are scrutinising the appropriateness of BCP to manage cyber risk when underwriting cyber insurance policies.

We have seen over 60% of Insurers now list Business Continuity Plans for Cyber Risk as one of the most critical topics in the determination of insurance policy pricing, capacity, and coverage. As claims continue to increase and the insurance market continues to harden, having formal BCPs for Cyber Risk will be a determining factor in how successful companies are in procuring competitive cyber insurance policies.

How 'Cyber Ready' is your BCM?

The Business Continuity Plans of two out of three companies are not 'Cyber Ready' for the challenges of the new digital economy or emerging disruptive cyber events.

44% Lack Business Continuity Management capabilities or Business Continuity Plans to mitigate financial losses from disruptive Cyber events

22% Have informal Business Continuity Plans that do not adequately or consistently address disruptive cyber events

26% Business Continuity Management strategy and Business Continuity Plans resources have been implemented to manage disruptive cyber events

8% Have an enterprise-wide approach to manage disruptive cyber events that incorporates advanced technology and practices.

The majority of manufacturing, retail, transportation and construction industries have the least 'Cyber Ready' approach to Business Continuity

48%

Manufacturing

Disruptive cyber exposures:

- Web-facing Operational Technology
- Industrial Internet of Things
- Enterprise Resource Planning systems

53%

Retail

Disruptive cyber exposures:

- Electronic Point-of-Sales devices
- e-Commerce solutions
- Inventory / Warehouse Management Systems

60%

Transportation and Logistics

Disruptive cyber exposures:

- Logistics / Supply Chain systems
- Compromised Integrity of HVAC/ IoT / Environmental Controls
- Warehouse Management System / Autonomous Picking technology

59%

Construction

Disruptive cyber exposures:

- Supervisory control and data acquisition (SCADA) / Programmable logic controller (PLC)
- Autonomous construction and maintenance vehicles (i.e. drones, trucks)
- Smart IoT building systems (i.e. lifts, locks, HVAC, BMS)

Four steps to 'upgrade' your BCM strategy for Cyber Risk

As the technology and threat landscape continues to evolve, it is important that the legacy Business Continuity Management (BCM) strategy is 'upgraded' to effectively mitigate financial loss and operational disruption to mission critical business activities.

Aon has identified four critical activities that could ensure your Business Continuity Management Strategies and Plans (BCPs) are aligned with business activities, critical technology assets and third party services.

1

Diagnose

Determine current readiness and maturity of the legacy Business Continuity Management strategy considers critical technology dependency and disruptive cyber threats.

2

Planning

Build Business Continuity Plans to explicitly address disruptive cyber risk scenarios to critical technology dependencies (internal systems and third party services)

3

Testing

Run tabletop exercises or full simulation exercises that contemplate disruptive cyber events to test the level of internal awareness and identify gaps in management strategies.

4

Governance

Develop an appropriate governance structure for the cyber-focused BCM strategy and BCPs to ensure these arrangements remain continuously tested and aligned with changes to the business model, technology infrastructure, and risk profile.

Find out more about how Aon can support you to 'upgrade' your BCM strategy for Cyber Risk click here

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com

Empower Results®