KPMG

apmaIAC Institute for Automotive Cybersecurity

Canadian automotive cyber preparedness survey

How well are auto parts manufacturers protecting their data against the new reality of cyber threats?

Today, our vehicles and workforces have become more connected than ever. In a COVID-19 world automotive manufacturers are faced with many challenges, not the least of which being the migration to the digital plain, where every electronic component is a potential point of vulnerability. Against this backdrop it has never been more important to answer the question: Is my organization cyber safe?

To help auto parts manufacturers find the answer and supercharge their defense mechanisms, KPMG in Canada and APMA's Institute of Automotive Cybersecurity joined forces in September 2020 to survey over 50 key industry players on their current actions, sentiments and plans for future preparedness. Below is a snapshot of the survey findings:

organizations have not changed their funding around digital transformation and cybersecurity initiatives, despite the impact of COVID-19

What type of problem is cybersecurity:

42% IT *vs* 58% business

DIGITAL CROWN JEWELS

The most mission critical data, processes, services and systems that, if compromised, would cause major business impact and disruption

Of the organizations that have identified their digital crown jewels, **54%** feel they are protected to a considerable or great extent

The extent to which auto manufacturers have a cyber strategy:

- **16%** No strategy
- **16%** In development
- **36%** Yes, within some areas
- **32%** Yes, across the entire organization

While **49%** of respondents indicate that their cybersecurity strategy leader is at the C-Suite level or equivalent

30% of organizations have experienced a breach in the last **12 months**

69% of auto manufacturers report having to comply with the cybersecurity controls of OEMs and other levels of their supply chain

13% say they don't have any designated individual driving their strategy at all

Top barriers to cyber preparedness

1. Lacking the right talent
2. Low visibility into the key risks
3. Lack of support from leadership
4. Unclear return on investment

78% of companies now have staff that operate on a work-from-home (WFH) basis

2 in 5 organizations have not conducted or are only in the process of planning for cyber preparedness testing

For more information or to secure a copy of the report, please email: **inquiries@kpmg.ca**

Read the full report:
December 2020

kpmg.ca