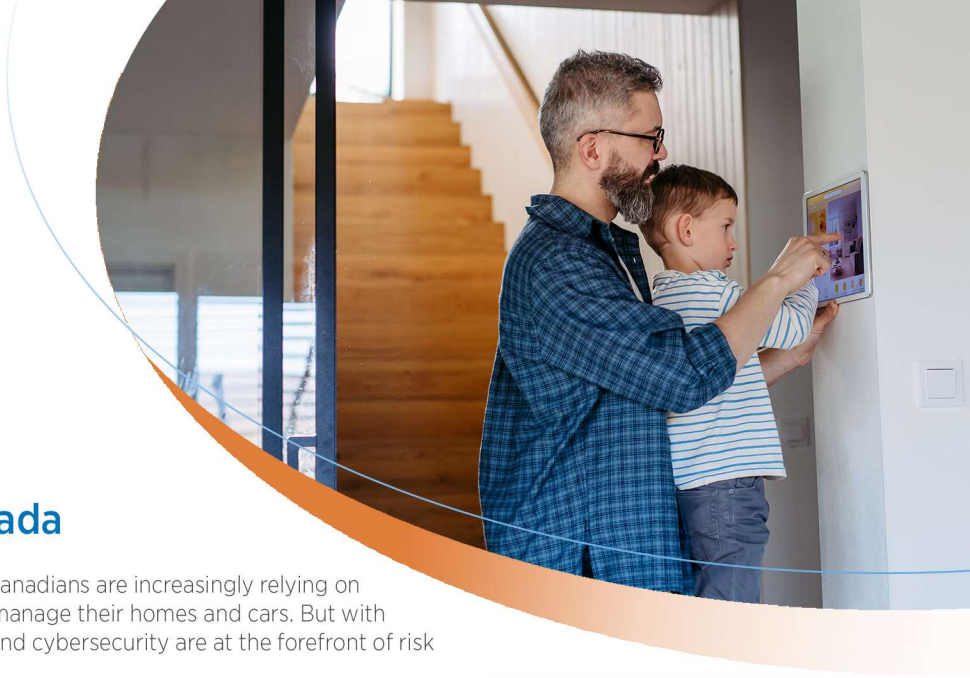
Gallagher

Insurance | Risk Management | Consulting



# Gallagher Insights

## Connected Cars and Homes: Navigating Cyber Threats in Canada

As digital technologies continue to reshape our daily lives, Canadians are increasingly relying on smart devices, connected vehicles, and online platforms to manage their homes and cars. But with convenience comes vulnerability. Artificial intelligence (AI) and cybersecurity are at the forefront of risk management for Canadian households and drivers.

### Growing cyber threats in Canada

Cybercrime continues to rise, impacting individuals as much as businesses:

- Canada experienced an estimated 116,700 to 164,648 cybercrime incidents in 2025.
- Canada costs in the country rose to approximately $220.5 billion in 2025, driven by ransomware.
- Ransomware remains the top cyber threat to Canadian organizations, 86.5% of Canadian organizations reported experiencing a cyber incident within the past year.

With more Canadians adopting smart thermostats, digital locks, and connected vehicles, personal exposure continues to increase.

### AI: Increasing risk and enhancing protection

AI has become a major factor on both sides of cybersecurity:

- Cybercriminals use AI to create deepfakes and launch persuasive phishing schemes.
- AI-driven security tools can detect threats 65% faster than traditional methods, offering real-time protection for homes and vehicles.

### Cyber risks in connected vehicles

Modern vehicles operate like mobile computers, creating new vulnerabilities:

- Infotainment, GPS, remote start, and telematics systems can be exploited if unsecured.
- AI-based diagnostics and data collection raise privacy concerns for drivers.
- Insurers are increasingly adopting AI for underwriting and claims, requiring strong data protection.

### Smart home cyber incidents: What can go wrong

Emerging threats show how AI-enabled attacks can directly impact homeowners:

- Deepfake scam: A homeowner receives a video call from what appears to be a distressed family member, actually an AI deepfake and shares access codes or transfers money.
  Potential claim: Theft or financial loss, depending on policy coverage.
- AI-powered phishing attack: Hackers send a highly convincing email from a "security provider," capturing login credentials and disabling alarms before breaking in.
  Potential claim: Stolen items and damages from the break-in.
- Fake AI-generated service requests: Criminals impersonate a homeowner to request lock or maintenance services, gaining unauthorized access.
  Potential claim: Stolen property and the cost of resecuring the home.

### How homeowners can protect themselves

- Use strong, unique passwords for all smart devices.
- Enable multi-factor authentication (MFA).
- Regularly update app, device, and firmware software.
- Verify all service providers and be cautious with unsolicited requests.
- Monitor smart home activity and alerts regularly.

### Cyber coverage for homes and autos

Gallagher offers tailored coverage, including cyber protection riders, that help clients recover from: Identity theft, Unauthorized system access, Digital property damage, Cyber-enabled theft or fraud.

**Sources:**

- Cybercrime Statistics in Canada 2025 – What You Need to Know
- National Cyber Threat Assessment 2025-2026
- The Canadian threat landscape is evolving. Here's what we found



**Request your quote online, or call us today:**

**888.336.7738**
pisales@ajg.com
**AJG.com/ca/opseu-sefpo/**

▶ Scan the QR code to request additional information about your exclusive group rate

Gallagher Go

***Gallagher Go — Canada**
Applied Systems Inc.

**Gallagher Go** is our powerful mobile home and auto insurance app, designed to give personal insurance clients quick and easy access 24/7 from wherever they are.