CYBERSECURITY
INCIDENT RESPONSE GUIDELINES

CYBERSECURITY - INCIDENT RESPONSE GUIDELINES*

- Security breaches - Caused by a network source, malware, spam, email scams, denial-of-service, social network interface, identity theft, mobile device interface.
- Common thread is securing your data environment.
- For a cybersecurity event, proper incident response mechanisms follow a common process.

- Do these in parallel:...perform these activities concurrently to ensure time-effectiveness!
  - **Get Support:** ...contact your IT department immediately.
  - **Update:** ...the software on your systems to repair unknown vulnerabilities and provide protection.
  - **Minimize:** ...disconnect effected devices, and potentially networks, from the Internet.
  - **Protect & Restore:** ...perform a full scan on effected systems using your updated Antivirus software.
    If infection(s) are found, consider system restore(s) of those instances.
  - **Inform & Educate:** ...inform your netowk users what has happened and what to do, and not do.
    Invoke new employee training for employees.
  - **Vigilance:** ...being alertly watchful, especially to avoid danger.
    Review & document the event's 5W's: Who, What When,Where & Why.
    Initiate appropriate actions to refine (or create) your incident response plan.
  - **Disclose & Report:** ...fully disclose the incident to help save others from experiencing similar issues.
    File a report with your local police department, and other law enforcement and/or regulatory officials.
  - **Reporting:** (See reverse side)
    Utilize Cybersecurity Incident Response Entities
    Fill out the Points of Contact (POC) Checklist

*Source: TMC RP537, Appendix IV (Proposed)

DG TECHNOLOGIES
Vehicle Network Solutions
CYBER TECH
248.888.2000
dgtech.com