How Lawyers' Mutual Insurance Company partners with leading and trusted experts to protect our members in the first 48 hours after a cyber incident

Preserve

- Take steps to preserve evidence for forensic investigation where possible
- Preserve firewall logs before they are over written
- Take at least one copy of the backups offline, if this has not been done already
- Switch to more secure communications (out-of-band)

Investigate

- Attempt to locate the ransom note, mark any threats of data leak and note the name of the group, if applicable
- Appoint a forensics investigator and provide forensics evidence
- Determine the scope of the attack
- Verify the viability of backups
- Appoint a lawyer
- Appoint a ransomware negotiator, if applicable

Minimize

- Consider isolating the affected environment until the situation is sufficiently contained
- Disconnect suspected compromised devices from the network
- Reset passwords for all accounts

Recover

- Establish a new way of working given limited capacity
- Form an action plan for a secure and quick recovery
  - Create a secure IT environment for recovering backups
  - Scan and assess newly restored backup for any sign of malware or cybercriminal activity
  - Install critical patches and limit services exposed to the internet

Claims handling and breach response services are provided by Beazley USA Services, a member of Beazley Group. Beazley USA Services does not underwrite insurance for Lawyers' Mutual Insurance Company. Policies purchased through Lawyers' Mutual Insurance Company are subject to Lawyers' Mutual's underwriting processes.
Source: Content provided by www.beazley.com. CYBER03_LMIC_Aug 2024