A SUITE OF COVERAGES **FOR BUSINESSES**

Computers, networks and electronic data are essential to managing farm operations and doing business, yet our reliance on these digital tools brings serious cyber risks like hacking and data breaches. Small and mid-sized businesses are particularly enticing targets for cyber thieves. Now more than ever, getting comprehensive cyber protection in place is critical for any business and farm operation.

Cyber Risk Protection Farm is a new, comprehensive coverage with multiple layers of insurance defense against the complex, ever-evolving cyber risks that businesses face every day. FMH is the among the first farm insurance companies to offer protection designed specifically for precision ag equipment and software.

WE'RE **HERE TO HELP**

As a business owner you count on us to protect you from today's cyber risks and challenges. For more information on Cyber Risk Protection Farm contact your FMH agent today.

Farmers Mutual Hail Insurance Company of Iowa

Farmers Mutual Hail
Insurance Company of Iowa

V2018.10.05 | 800067

Farmers Mutual Hail Insurance Company of Iowa

Farmers Mutual Hail
Insurance Company of Iowa

CYBER RISK PROTECTION
FARM

COVERAGE, TERMS, AND CONDITION **HIGHLIGHTS**

Cyber Risk Protection Farm includes five available coverages to help businesses affected by data breaches and cyber attacks:

Data Compromise Response Expense
Coverage designed to provide the resources to respond to a breach of personal information.

Computer Attack
Coverage designed to provide resources to respond to a computer attack.

Cyber Extortion
Coverage designed to respond to an extortion threat.

Data Compromise Liability
Coverage designed to provide defense and settlement costs in the event of a suit related to a breach of personal information.

Network Security Liability
Coverage designed to provide defense and settlement costs in the event of a suit alleging that a system security failure on the part of the insured caused damage to a third party.

ADDITIONAL SERVICES

Your business will have access to these other services:

- Access to eRiskHub®, a risk management portal designed to help business owners, like you prepare and respond effectively to data breach and cyber attacks. Key features of the eRiskHub® portal include: an incident response plan roadmap, online training modules, risk management tools to manage data breaches, a directory for external resources, a news center with current articles from industry resources, and a learning center with best practices and tips
- Access to "TechQ" which offers FREE computer diagnostics by phone and competitive rates for virus removal, technical assistance, and related digital security services
- Access to experts in recovering from cyber extortion and data breaches
- Claims managed by experienced and dedicated cyber claim specialists with industry knowledge

CLAIM EXAMPLES

Scenario 1 - Computer Attack
A seed dealer's computer was hacked, compromising payment and personal client data. The seed dealer's clients were from multiple states and he needed assistance in meeting the various notification requirements under each state's law. Clients were urged to contact their banks and place fraud alerts on their credit files.

Scenario 2 - Compromised Data
A burglar broke into a farmer's office and stole a computer with the private information and tax records of their employees. The insured consulted with an attorney specializing in data breach and notifications were sent to the affected employees advising them to place a fraud alert with credit bureaus and to monitor their credit reports and other financial statements.

Scenario 3 - Cyber Extortion
An insured's employee on a dairy farm opened a file in an email causing the dairy's computer systems including production data, to become encrypted. The insured received a message stating that in order to receive the decryption key, he needed to pay a ransom in bitcoin. If the ransom was not received within a week the key would be destroyed and any chance of accessing his files would be lost forever. The insured consulted with his carrier and they determined that the threat was credible. A negotiator was hired and the extortion was paid.