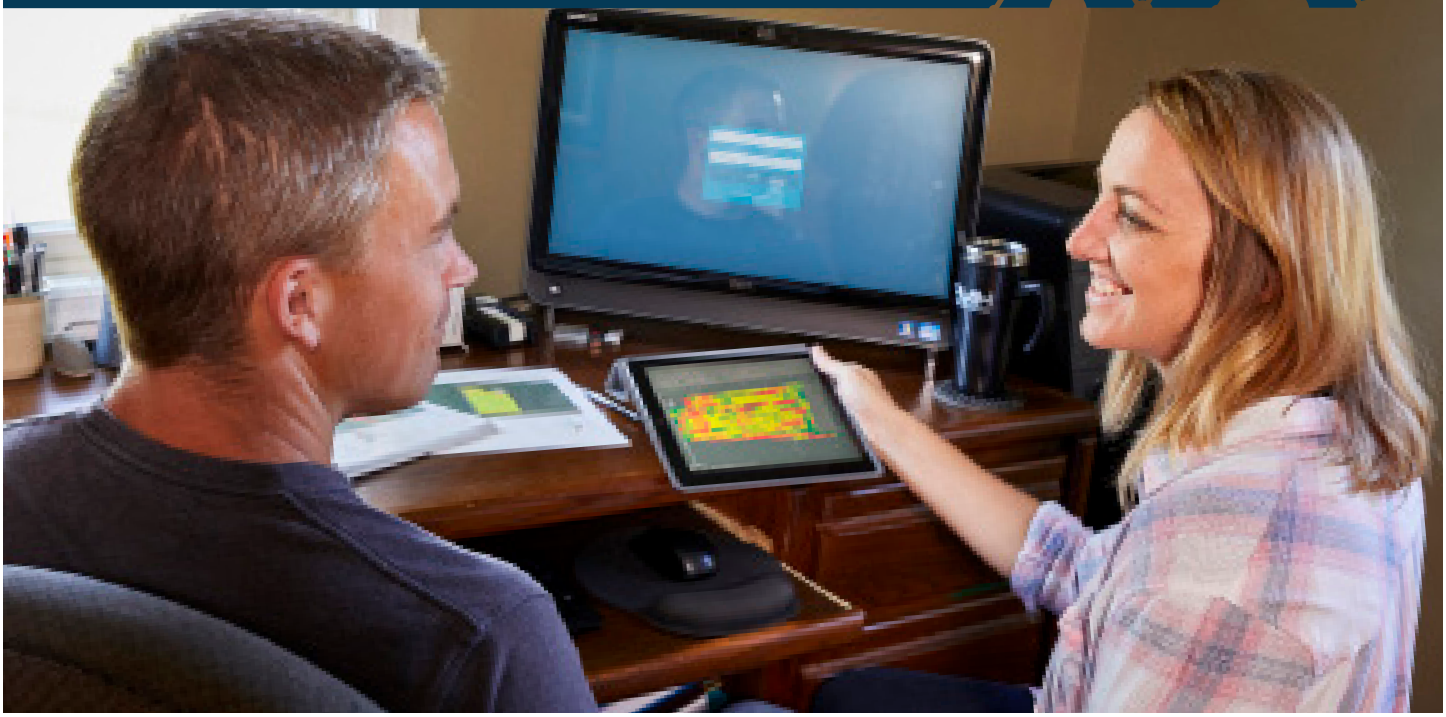
# CYBER RISK PROTECTION HOME
# **FAQs & CLAIM SCENARIOS**



## WHAT IS **CYBER RISK PROTECTION HOME COVERAGE?**

Our Cyber Risk Protection Home coverage is a suite of coverages and services built to respond to computer and home system attacks, cyber extortion, online fraud, and the breach of personal information involving smart phones, computers and connected home devices.

### Who needs this coverage?

Individuals and families who are looking to protect themselves from problems created by an increasingly connected world.

### Who is eligible for coverage?

Dwelling policyholders are eligible.

### Why is this coverage needed?

Privacy and security are major concerns for homeowners and renters, and many individuals and families are looking for a way to protect that privacy and security with meaningful, reliable insurance. This concern is growing quickly for several reasons:

- Growth in connected home technology and smart devices has created the increased need to protect data, systems, and software from computer attacks.
- Criminal activities – like cyber extortion and online fraud – also threaten homeowners and renters with financial loss.
- Just as with commercial entities, people who hold non-public personal information of others may have notification requirements and other obligations under state law if that information is lost or stolen.

### Our Cyber Risk Protection Home coverage goes beyond any personal cyber insurance available by combining coverage for:

- Computer attack
- Home systems attack
- Cyber extortion
- Online fraud
- Data breach
- Identity Recovery

Farmers Mutual Hail Insurance Company of Iowa

## What coverages are included?

Payments to recover data and restore systems that have been lost or damaged due to a cyberattack – including attacks involving malware or the unauthorized use of owned or leased computers, mobile devices, and connected home devices

- Professional assistance in responding to cyber extortion demands based on credible threats to damage, disable, deny access to or disseminate content from devices, systems or data
- Online fraud protection that results in a direct financial loss to a covered policyholder
- Notification and payment for services to affected individuals in the event that private personal data entrusted to a household resident is breached
- Payments for the costs to help individuals respond to identity theft, coverage for out-of-pocket expenses, services of a case manager, access to a professional restoration firm to assist with the identity restoration process, and a toll free identity helpline to educate insureds about identity theft preventative measures and tips

## When is coverage triggered?

Depending on the coverage element, coverage can be triggered by the insured's discovery of a cyberattack, cyber extortion threat, online fraud event, data breach, or identity theft. It is a requirement that the triggering event be discovered during the policy period and reported within 60 days. Certain exclusions may apply as described in the policy.

## How is coverage added for my insureds?

Coverage is available as an enhancement by way of an endorsement to a dwelling policy.

## How do I get a quote for my insureds?

Contact your FMH underwriter or online quoter.

## Is an application or other data required for a quote?

No separate application is needed.

## What limits and deductible options are available?

Coverage limit options $15,000 and $25,000 per policy annual aggregate limit. $500 deductible per occurrence. Identity recovery coverage is subject to $0 deductible.

# **CLAIM** EXAMPLES

### Scenario 1 - Cyberattack

An insured opened a file in an email she received and the email unleashed a virus. In addition, the virus infected the computer, forcing the insured to hire an outside expert to reformat the hard drive, reinstall the operating system and all the software, and restore data from the backup.

**Total Paid Loss: $1,200**

### Scenario 2 - Extortion

An insured received a ransom note on his computer after he noticed his files were locked. The email informed him that the files were encrypted and to obtain the decryption key he needed to pay $2,000. If the insured failed to pay within the week, the price would go up to $3,000. After that his decryption 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 payment was advisable.

**Total Paid Loss: $2,000**