



## Building a Community of Cyber Resilient Insureds

### Program Overview

The **Fusion InsurSec 360** program is a step forward in the combination of **Proactive & Reactive** approaches to risk management by providing **both** Insurance and Tools to improve the policyholder's exposure.

An innovative and comprehensive Insurance program complemented by the **FusionHub** platform provides **360 Degrees of Protection** before and after the claim.

- ✓ Cyber Program & Risk Management for businesses up to **\$750M in revenue**
- ✓ Product is **Available Nationwide** on Non-Admitted paper through Lloyds of London
- ✓ Digital product with Quote, Bind, and Issue functionality with **Limits up to \$5,000,000**
- ✓ Access to the **FusionHub** Risk Management platform, including Fusion Security Tools
- ✓ Claims handled by CyberClan and TMK Incident Response Team

### Product Highlights

#### Coverage Benefits

- Limits available from \$500,000 to \$5,000,000
- Full Limit available for Cyber Extortion, Dependent Business Interruption, Dependent System Failure, Bricking, Betterments, and Cryptojacking
- Cyber Crime to include: Theft of Funds in Escrow, Corporate Impersonation, and Theft of Goods Enhancements include: Reverse Social Engineering, Voluntary Shutdown, and Pay On Behalf Language
- No Cyber Crime callback provision in the policy
- 23% Commission

#### Fusion's Approach to Cyber Risk Management

Helping Users become intimately aware of the phishing threat landscape is the best way to prevent cyber events from occurring. **It's where 75% of all cyber events start.**

That's why we include our **Phishing Simulation (FusionPhish)** exercises to all Insured's at **no additional cost**. Additionally, it initiates immediately without any action required of the Insured.



**FusionPhish** uses a variety of techniques to simulate phishing attacks, just like real attackers do. Users will receive knocks that range from seemingly obvious scams, to deceptively advanced phishing attempts that mimic the sophisticated nature of the new wave of cyber-criminals.

Users who engage with these simulated attempts will receive a notice explaining what happened, and refer them to resources for additional training. If a user consistently engages with simulated phishing attempts, the cyber insurance contact will also be notified.