FLTA Recommended Cyber Security Best Practices

Purpose: Cyber fraud and crime have become prevalent in the real estate market and title underwriters, agents and their customers are being victimized daily. Cyber criminals are generally targeting escrow funds and data held by the Company. There is no "one size fits all" approach to cyber security. The Company's approach to combatting cyber fraud and crime should be appropriate to the Company's size and complexity and the nature and scope of the Company's business and activities. However, regardless of the Company's size and complexity, it is important to take cyber threats seriously, create a multi-layered and enterprise-wide approach, and continually review with, train, and test employees, systems, and processes.

The suggestions below represent principles and applications for consideration when creating a cyber security plan – it all starts with: **S**etup, **T**rain, **O**btain and **P**lan – in essence, the word: **STOP.**

S – Set up appropriate processes and controls to protect the Company and Consumers from Cyber Fraud

- People
    - Create processes and procedures to prevent cyber fraud, which might include use of:
        - Encryption of information on the Company's servers
        - Encryption of email communications
        - Strong passwords
        - VPNs when working remotely
        - VPNs when using unsecured Wi-Fi networks
        - Multifactor authentication
        - Dual authorization for initiating and releasing wires
        - Appropriate records retention and data protection practices
        - Communication of the Company's cybersecurity practices with its customers and business associates
    - Create processes and procedures for identifying cyber fraud when it is attempted, which might include:
        - Prohibiting changes to wire instructions
        - Independent verification of wire instructions
        - Installation of email filters that identify suspicious emails and prevent users from opening them without first being identified as safe
        - Monitoring systems for intrusion and data breach
        - Independent verification of both the initial payoff instructions and then receipt of funds
    - Educate employees on the Company's processes and procedures as well as the risks and consequences of cyber fraud and the employees' important role in preventing and mitigating it
    - Train employees how to recognize cyber fraud and what to do when they see it
    - Provide regular and consistent testing to assure employees are following the established processes and procedures
- Systems
    - Use of firewalls

- Installation and regular and timely updating of anti-virus and malware software on all computers
- Implementation of intrusion prevention protocols, which might include:
  - Restrictions on internet usage and downloads
  - Lock down of physical computer ports
- Installation and setup of appropriate email spam and phishing filters
- Use of VPNs
- Regular and frequent backups of Company systems and data
- Regular and timely patching and updating of Company systems
- Performance of penetration tests and vulnerability assessments

- Purchase appropriate cyber and crime insurance coverage (in scope and amount)
- Create a WISP (Written Information Security Plan)
- Create a WIRP (Written Incident Response Plan)

T- Train and Educate Staff, Clients and Consumers

- Train and Educate Staff:
  - Periodic and consistent training on Cyber Security
    - Establish an internal Cyber Security Committee
    - Establish phish campaigns with a testing component
    - Regular and frequent reminders of the importance of cyber security vigilance
- Train and Educate Clients and Consumers:
  - Educate the Consumer on their role in cyber security on topics, which might include:
    - Wire Fraud
    - Non-Public Personal Information/NPI Security
    - Email Security
    - Password Security
    - Phishing, spoofing, ransomware and other malicious clickbait
    - Verifying that all communications received came from the authentic source
  - Obtain a written acknowledgement from Consumer that they received and understand Company's listed cyber security protocols and practices
  - Introductory phone call at the beginning of the transaction

O- Obtain and maintain appropriate insurance and cyber coverage.

- Seek counsel of a trusted insurance agent that understands your business to explain coverages/exclusions
- Understand your insurance needs (coverages, amounts, etc.) based on your business model
  - E&O insurance – What does and doesn't it cover and what to look for:
    - Cyber coverage is excluded in all E&O policies (there are some optional supplements that can be added but this is not full cyber coverage)
    - Wire fraud is not covered under E&O
  - Fidelity/Crime – What does and doesn't it cover
  - Cyber – What does and doesn't it cover and what to look for:
    - Social Engineering/Fraudulent Impersonation coverage
    - Bricking coverage (replacement of unusable hardware after a cyber-related event)

        - Ransomware coverage
    - Financial stability/strength of your insurer

P – Plan for the worst. Establish written plans to anticipate and promptly respond to cyber-related incidents.

- Create a Written Information Security Plan (WISP) that:
    - Identifies and implements effective administrative, technical and physical safeguards
    - Secures the confidentiality of personal information of consumers and employees
    - Protects personal information (NPI) and identifies procedures for evaluating electronic and physical methods of:
        - Access
        - Collection and Transmission
        - Storage
        - Use

- Create a Written Incident Response Plan (WIRP) to identify and implement effective processes and procedures for responding to a cyber-theft of money or data
    - Possible areas for consideration might include:
        - Establishment of an internal response team (IRT)
        - List of persons to contact based on the incident
        - Securing of the Company's office and network
        - Document specifics of breach or loss
        - Retain experts to assist with recovery/restoration efforts where necessary
        - Test Company's WIRP for effectiveness (what did we learn?)
        - Review and update Company's WIRP regularly