Top Cybersecurity Challenges for mREIT Companies

In the increasingly complex landscape of cyber threats, no industry is safe. While major financial institutions were once a primary target for cyber attacks, hackers are shifting their focus to more lucrative opportunities. Mortgage real estate investment trust (mREIT) firms have emerged as enticing targets due to their vast repositories of underlying loan information, investor and employee data. A single breach can cripple operations, undermine trust and financially devastate a business.

Top 9 Security Challenges for mREITs

1. Regulatory Compliance

THE CHALLENGE: mREITS are subject to stringent cybersecurity regulations and State Privacy laws, including the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), California Consumer Privacy Act (CCPA) and New York SHIELD Act. Failure to comply can result in significant fines and penalties.

THE SOLUTION: Implement a regulatory compliance management framework, such as NIST CSF or NIST 800-53, do regular assessments against the associated controls and put a plan in place to address any gaps.

2. Third-party Vulnerabilities

THE CHALLENGE: Your vendors may have access to your business’s sensitive data. If these partners don't uphold stringent cybersecurity standards, that data becomes vulnerable to significant risk.

THE SOLUTION: Conduct frequent third-party risk assessments to identify, evaluate and mitigate your risk exposure. Determine which vendors are critical to your operations and your supply chain and identify back-up suppliers in the event they are no longer able to provide services.

3. Lack of Employee Awareness

THE CHALLENGE: mREIT employees may not be adequately equipped or educated on the latest cyber threats or cybersecurity protocols, which opens the door for cyber-hackers to find their way in. In fact, human capital is generally considered the weakest link and a major security risk in any organization.

THE SOLUTION: Provide ongoing cybersecurity awareness training and support resources to employees. Train all new employees as they join the organization.

> *In fact, human capital is generally considered the weakest link and a major security risk in any organization.*

4. Business Email Compromise (BEC)

THE CHALLENGE: Cyber criminals are getting savvier at mimicking executives or vendors via email to trick employees into approving fraudulent transactions or revealing confidential data—and more are employees are falling for it.

THE SOLUTION: Invest in holistic employee cybersecurity training that includes a robust deep dive into how phishing campaigns work and how to avoid falling victim to such scams.

5. **Ransomware Threats**

THE CHALLENGE: mREITs generally store large amounts of sensitive data, making them especially vulnerable to cyberattacks; particularly ransomware. Encryption alone can lead to costly and delayed data recovery.

THE SOLUTION: Implement a robust backup strategy, regularly test your backups, and educate employees on ransomware threats.

> *mREITs generally store large amounts of sensitive data, making them especially vulnerable to cyberattacks; particularly ransomware.*

6. **Exposure Related to Remote Work**

THE CHALLENGE: The profound rise in remote work has ushered in a new wave of cybersecurity challenges for the industry. As more employees connect using personal devices and networks, the potential for a breach multiplies.

THE SOLUTION: Create, implement and communicate cybersecurity policies and procedures and require adherence by all employees.

7. **Cybersecurity Talent Shortage**

THE CHALLENGE: Cyber attackers' ever-changing and increasingly sophisticated approaches, have created a shortage of skilled cybersecurity professionals; maintaining a robust security program is becoming more of a challenge. This deficiency can weaken your ability to proactively defend against security breaches and swiftly respond when one occurs.

THE SOLUTION: Outsource certain cybersecurity functions to a third-party expert or train existing staff members to bridge this gap. Also, consider implementing an automation solution with AI to instantly separate real threats from the noise.

8. **Legacy Systems**

THE CHALLENGE: If your business still relies on legacy technology to power operations, it is highly susceptible to modern threats. These outdated systems are likely not operating with the latest security updates, software, or patches.

THE SOLUTION: Modernize your applications, conduct vulnerability assessments, and implement frequent/regular security patches to reduce the risks associated with your legacy technology.

9. **API Vulnerability**

THE CHALLENGE: Your business likely relies heavily on software applications and APIs for financial transactions. If these APIs are inadequately secured, they are exploitable targets for cyber attackers.

THE SOLUTION: Ensure your applications have a solid architecture design. This will inherently boost the security of your APIs.

Your ability to respond swiftly and effectively can mean the difference between a managed incident and a catastrophic fallout. By implementing the solutions outlined above, you will enhance your organization's resilience against cyber threats, safeguard critical assets and instill greater confidence in your stakeholders and clients.

For more information about how we can help you navigate the complex cybersecurity risks facing mREIT firms, contact us here.