Author
Melinda Yerkes

Cybersecurity and Data Protection

One Rose Consulting, LLC

MORTGAGE LICENSING &
COMPLIANCE MADE EASY!

CYBERSECURITY & DATA PROTECTION:

Safeguarding Borrower Data and Regulatory Trust

Author:
Melinda Yerkes

WHY CYBERSECURITY IS NOW A TOP REGULATORY PRIORITY

Cybersecurity is no longer an IT issue — it is a core compliance obligation. Mortgage companies handle vast amounts of highly sensitive consumer information, making them prime targets for cybercrime, data breaches, and identity theft.

State and federal regulators now expect mortgage companies to implement robust information security programs that **protect borrower data**, **prevent unauthorized access**, and e**nsure business continuity**.

At One Rose Consulting LLC, we often remind our

> ***Cybersecurity failures are compliance failures.***

THE REGULATORY LANDSCAPE GOVERNING CYBERSECURITY

Mortgage companies are subject to a growing number of cybersecurity regulations, including:

- **FTC Safeguards Rule (16 CFR Part 314)**
- **NYDFS Cybersecurity Regulation (23 NYCRR Part 500)**
- **State privacy and data protection laws**
- **GLBA (Gramm-Leach-Bliley Act)**
- **State examination cybersecurity programs**

Failure to comply can result in severe penalties, enforcement actions, civil liability, and repuational harm.

WHAT REGULATORS EXPECT FROM A CYBERSECURITY PROGRAM

Regulators expect mortgage companies to maintain a formal Written Information Security Program (WISP) that includes:

- Risk assessments
- Written policies and procedures
- Access controls
- Data encryption
- Vendor oversight
- Incident response planning
- Business continuity and disaster recovery
- Employee training

Cybersecurity is evaluated not only by the presence of policies, but by documented implementation.

CORE COMPONENTS OF AN EFFECTIVE CYBERSECURITY PROGRAM

1. Written Information Security Program (WISP)

A comprehensive WISP establishes governance, risk management, controls, monitoring, and accountability.

2. Risk Assessments

Annual risk assessments identify vulnerabilities, threats, and control gaps, forming the foundation of cybersecurity strategy.

3. Access Controls & Authentication

Strong access protocols, multi-factor authentication, and least-privilege principles reduce unauthorized system access.

4. Data Encryption & Secure Transmission

Encryption protects borrower data both at rest and in transit.

5. Vendor & Third-Party Oversight

Companies must assess cybersecurity risks posed by vendors and service providers.

6. Incident Response Planning

Documented response plans ensure rapid containment and regulatory notification in the event of a breach.

7. Business Continuity & Disaster Recovery

BCDR planning ensures operational resilience during system outages or cyber incidents.

8. Employee Security Awareness Training

Employees remain the largest cybersecurity vulnerability. Ongoing training is essential.

COMMON CYBERSECURITY WEAKNESSES REGULATORS FIND

Regulators frequently identify the following deficiencies:

- Missing or outdated WISP
- No formal risk assessments
- Weak access controls
- Lack of vendor due diligence
- No incident response plan
- No cybersecurity training
- Weak backup and recovery procedures

Any of these gaps may result in immediate corrective action demands.

HOW CYBERSECURITY FAILURES IMPACT MORTGAGE COMPANIES

Cybersecurity incidents often result in:

- Regulatory enforcement
- Consumer litigation
- Financial penalties
- Loss of investor confidence
- Reputational damage
- Business interruption

Strong cybersecurity controls reduce both operational and regulatory risk.

THE ORC CYBERSECURITY COMPLIANCE FRAMEWORK

One Rose Consulting LLC provides a comprehensive cybersecurity compliance framework tailored to mortgage industry risk.

Our framework includes:

1. Cyber Risk Assessment
2. Policy Development & Updates
3. Technical Control Evaluation
4. Vendor Risk Management
5. Employee Training Programs
6. Incident Response Planning
7. Regulatory Compliance Mapping

CYBERSECURITY READINESS CHECKLIST

Use this checklist to evaluate your organization's cybersecurity posture:

- ✓ **WISP current and compliant**
- ✓ **Annual risk assessment completed**
- ✓ **Multi-factor authentication enabled**
- ✓ **Data ecryption implemented**
- ✓ **Vendor cybersecurity reviews completed**
- ✓ **Incident response plan documented**
- ✓ **Disaster recovery tested**
- ✓ **Employee training completed**

WHY PROFESSIONAL CYBERSECURITY COMPLIANCE MATTERS

Professional cybersecurity compliance provides:

- Reduced breach risk
- Lower regulatory exposure
- Faster incident recovery
- Improved investor confidence
- Long-term business resilience

HOW ONE ROSE CONSULTING LLC SUPPORTS CYBERSECURITY COMPLIANCE

Our cybersecurity compliance services include:

- Risk assessments
- Policy development
- Vendor risk management
- Employee training
- Regulatory compliance support
- Examination readiness

LICENSING & COMPLIANCE MADE EASY!

One Rose Consulting, LLC

MORTGAGE LICENSING & COMPLIANCE MADE EASY!

727-291-0790

WWW.ONEROSECONSULTING.COM