

STRENGTHEN YOUR CYBERSECURITY PROGRAM

A strong cybersecurity program does more than protect your organization. It also helps position you more favorably with cyber insurance carriers. Implementing these best practices can help reduce risk, minimize disruption, and support more competitive coverage terms.

TRAINING & AWARENESS

Ensure employees are regularly trained to recognize cyber threats and respond appropriately.

Key Practices

- Mandatory annual cybersecurity awareness training
- Annual phishing simulations with measurable results

Next Steps

Leaders should require a formal training program with reporting that shows employee participation, testing outcomes, and year-over-year improvement.

EMAIL & ACCESS SECURITY

Protect email systems and critical accounts from unauthorized access and social engineering attacks.

Key Practices

- Advanced email security, including SPF, DKIM, and DMARC
- Multi-factor authentication (MFA) for remote access and critical systems
- Privileged access management (PAM) for administrative accounts

Next Steps

Leaders should confirm that strong email protections and MFA are fully enforced, especially for privileged and business-critical access.

ENDPOINT & VULNERABILITY MANAGEMENT

Continuously identify, monitor, and remediate weaknesses across devices and systems.

Key Practices

- Ongoing vulnerability scanning and timely patching
- Periodic penetration testing
- Endpoint detection and response (EDR) across company assets

Next Steps

Leaders should hold IT and security teams accountable for documented patching timelines, testing results, and endpoint protection coverage.

MONITORING & THREAT DETECTION

Maintain around-the-clock visibility into suspicious activity to detect and respond to threats quickly.

Key Practices

- 24/7 security monitoring through a SOC and/or SIEM

Next Steps

Leaders should ensure the organization has continuous monitoring in place, whether internally or through a qualified third party.

QUESTIONS?

Conner Strong & Buckelew's Cyber Practice Group closely monitors emerging threats and trends to support our clients. Please reach out to your account representative or call us at 1-877-861-3220 with any questions.



DATA PROTECTION & BACKUP

Protect sensitive information and ensure critical systems and data can be restored after an incident.

Key Practices

- Secure, protected backups
- Annual backup restoration testing
- Data loss prevention (DLP) tools

Next Steps

Leaders should require proof that backups are secure, recoverable, and tested regularly to support business continuity.

GOVERNANCE & THIRD-PARTY RISK

Establish formal oversight of cyber risk, including vendors, frameworks, and asset management.

Key Practices

- Third-party security assessments
- Alignment to a recognized framework such as NIST CSF or ISO 27001
- Automated asset inventory and lifecycle management

Next Steps

Leaders should adopt a formal governance framework and require visibility into vendor risk, asset inventory, and unsupported systems.

INCIDENT RESPONSE & RESILIENCE

Prepare the organization to respond effectively to cyber events and recover with minimal disruption.

Key Practices

- Formal incident response planning and testing
- Business continuity and disaster recovery planning with defined recovery objectives

Next Steps

Leaders should sponsor and test incident response and recovery plans so the organization can act decisively during a cyber event.

ADVANCED & EMERGING RISKS (AS APPLICABLE)

Address evolving exposures tied to new technologies and operational environments.

Key Practices

- AI governance for critical operations
- IT/OT segmentation where applicable

Next Steps

Leaders should evaluate emerging technology risks and require appropriate controls before those exposures impact operations.

CONNER
STRONG &
BUCKLEW