McKONLY & ASBURY

The Financial Executive's Guide to Cybersecurity

macpas.com

Firm Overview

Helping You Thrive!

McKonly & Asbury

M&A is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

accountingTODAY 2025 Best Firms to Work For

accountingTODAY 2025 Best Firms for Young Accountants

BEST PLACES to work in PA 2025

Services Provided

- Advisory & Business Consulting
- Audit & Assurance
- Tax
- Entrepreneurial Accounting Solutions
- SOC & Technology Consulting

Industries Served

- Affordable Housing
- Architecture, Engineering, and Construction (AEC)
- Entrepreneurial
- Family-owned Business
- Franchises
- Healthcare
- Manufacturing & Distribution
- Nonprofit
- Public Companies

Executive Summary

Cybersecurity is no longer just an IT issue—it is a financial, operational, and reputational risk.

Protect Assets

- Finance leaders help protect company assets and reduce loss exposure.

Ensure Compliance

- Finance leaders support compliance and audit readiness.

Build Trust

- Finance leaders help maintain customer, investor, and stakeholder trust.

Agenda for Our Conversation

- Why Cybersecurity matters to the Financial Executive
- Key terms you should know and what they mean
- Significant controls to have in place
- Your role in cyber-risk mitigation
- Practical first steps

McKONLY & ASBURY

Why Cybersecurity Matters to Finance

Why Cybersecurity Matters to Finance

The Financial Reality (2024-2025 Data)

$4.9 M	Average cost of a data breach	IBM, 2024
$5.1M	Average total cost of a ransomware attack	including downtime & recovery
Up to $125K/hour	Operational downtime cost	industrial and service businesses
~$2.8M per incident	Lost business — largest cost category	revenue, customers, reputation
~1.9% of annual revenue	Average financial impact of cyber incidents	*Reuters* reporting

Why Cybersecurity Matters to Finance

What Drives the Cost (Beyond IT)

- Business interruption & lost production
- Customer churn and reputational damage
- Legal, regulatory, and notification costs
- Extended recovery timelines (often months)

McKONLY & ASBURY

Common Language – Key Terms and Data Points

Common Language: Key Terms and Data Points

- Types of Cyber Threats to Consider
- Cybersecurity Frameworks & Compliance Requirements
- Significant Metrics

Key Cyber Threats

- **Business Email Compromise (BEC)**
  - Fraud using spoofed or hijacked email accounts
- **Ransomware attacks**
  - Malware that encrypts systems and demands payment
- **Data breaches**
  - Unauthorized access to sensitive company or customer data
- **Third-party/vendor risk**
  - Exposure through partners, suppliers, or service providers
- **Insider threats**
  - Risks from employees or contractors (intentional or accidental)

Cybersecurity Frameworks & Compliance

- **NIST Cybersecurity Framework**
  - Widely used U.S. risk management framework
- **SOC 2**
  - Third-party assurance report for service organizations
- **ISO 27001**
  - Global standard for information security management systems
- **CMMC / NIST 800-171**
  - Mandatory requirements for U.S. Department of War contractors
- **Alignment with SOX/internal controls**
  - Integrating cybersecurity into financial control environment

Metrics and Reporting

- **Number of incidents**
  - Measures overall exposure and attack frequency
- **Time to detect/respond**
  - Measures speed of identifying and containing threats
- **Vulnerability status**
  - Measures known weaknesses in systems and applications
- **Access risks**
  - Measures control over who can access critical systems and data
- **Financial impact reporting**
  - Translates cyber events into business terms

McKONLY & ASBURY

Core Controls to Have in Place

Core Controls to Have in Place

- **Segregation of duties**
  - Prevents any single individual from having end-to-end control
- **Multi-factor authentication (MFA)**
  - Adds a second layer of identity verification beyond passwords
- **Verification of payment changes**
  - Controls against vendor fraud and Business Email Compromise (BEC)
- **Regular access reviews**
  - Ensures employees only retain appropriate system access
- **Transaction monitoring**
  - Detects unusual or suspicious financial activity

Controls: Perception vs. Reality

Control	Expected	Reality
Segregation of Duties	Formal separation across finance and system access	Overlapping access in ERP, finance, and admin systems
Multi-Factor Authentication (MFA)	MFA enforced everywhere sensitive data exists	Partial coverage; exceptions for legacy systems or vendors
Payment Change Verification	Strict out-of-band verification for all vendor banking changes	Informal email-based approvals still common in AP workflows
Access Reviews	Quarterly or automated entitlement reviews	Infrequent, manual, or inconsistently enforced reviews
Transaction Monitoring	Real-time or near real-time anomaly detection	Post-transaction review or limited rule-based alerts

McKONLY & ASBURY

The Financial Executive's Role

The Financial Executives Role

- Leadership and Communication
- Championing a Security Aware Culture
- Managing Third-party Vendor Risk
- Budgeting and Investment Strategy
- Integration with CIO / CISO

Role 1: Leadership & Communication

- **Translate cyber risk into financial terms**
  - Share broadly, at all levels of leadership
- **Ensure appropriate budgeting**
  - Cyber-Risk-Management spend is not optional
  - Must be strategic, thoughtful and forward looking
  - Defend the spend by presenting ROI
- **Oversee internal controls**
  - Design AND Operating Effectiveness
- **Report risks to board and audit committee**
  - Board priorities must include managing cyber risk

Role 2: Champion a Security-Aware Culture

- **Security awareness training**
  - Establishes baseline employee understanding of cyber risk
  - Ongoing, not just annual!
- **Phishing prevention**
  - Primary defense against credential theft and account compromise
- **Payment fraud controls**
  - Protects against Business Email Compromise (BEC) and wire fraud
- **Leadership example**
  - Sets tone from the top for security behavior
  - No special treatment!
- **No-Blame Reporting**
  - Encourages employees to report suspicious activity immediately

Role 3: Manage 3rd Party / Vendor Risk

- **Vendor due diligence**
  - Assess security before granting access or sharing data
- **Review SOC 2 reports**
  - Validate independently audited security controls
- **Ongoing Vendor Risk Monitoring**
  - Risk is dynamic—not a one-time assessment
- **Include security clauses in contracts**
  - Legally enforceable cybersecurity expectations

Role 4: Budgeting & Investment Strategy

- **Treat cybersecurity as risk management**
  - Align spending to financial exposure, not technical preference
  - Prioritize investments based on likelihood × financial impact of risk
  - Shift mindset from “IT expense” to **loss prevention strategy**
- **Invest in Core Security Controls (Highest ROI Areas)**
  - Focus on foundational protections that reduce most common attack paths
    - *Identity & Access Management (IAM):* controls access to systems and data
    - *Endpoint security:* protects devices from malware and intrusion
    - *Backups & recovery:* ensures business continuity after ransomware or outage

Role 4: Budgeting & Investment Strategy

- **Evaluate cyber insurance strategically**
  - Transfer a portion of residual risk—but do not rely on it alone
  - Requires strong baseline controls (MFA, backups, access controls) to qualify
  - Warning: Policies vary significantly in exclusions and coverage limits
  - Best viewed as **risk transfer, not risk elimination**
- **Measure ROI through risk reduction**
  - Justify investment using avoided loss, not just cost
  - ROI is realized as **losses that did not occur**

Role 5: Integration with the CIO/CISO

- **Unified View of Enterprise Risk**
  - Cyber risk is financial risk in operational disguise
- **Smarter Capital Allocation**
  - Align cybersecurity investment with financial exposure
- **Faster, More Effective Incident Response**
  - Financial decisions are embedded in cyber response
- **Improved Governance & Board Reporting**
  - Clear, consistent risk communication to leadership
- **Stronger Control Accountability Across the Organization**
  - Cybersecurity becomes embedded in business processes

McKONLY & ASBURY

Next Steps

Practical First Steps

- **Conduct a risk assessment**
- **Start with the most significant areas**
  - Strengthen payment controls
  - Implement MFA
  - Validate backups
  - Strengthen vendor management controls
- **Review your cyber insurance**
  - Understand policy exclusions and what costs / activities it *actually* covers
- **Align with a framework and begin / enhance documentation**

Final Thoughts

- Cybersecurity is a business risk with clear financial consequences.
- Active CFO engagement strengthens resilience, oversight, and trust.
- Start with practical controls, measurable metrics, and ongoing partnership with IT/security.
- View security-related costs as an investment with an ROI, not as an income statement expense by ‘necessity’ or capital outlay.

McKONLY & ASBURY

Michael Hoffner
Managing Partner
mhoffner@macpas.com
717.972.5756

David Hammarberg
Partner
dhammarberg@macpas.com
717.972.5723

macpas.com