

REGULATORY UPDATE

Working Together. Evolving Together.

The Holt Group

CYBER | RISK MANAGEMENT

Cyber Risk in 2026: Strong Controls Matter More than Ever

Evolving Threats, Social Engineering and Underwriting Expectations are Keeping Cyber Resilience in Focus

CURRENT ENVIRONMENT	PRIMARY EXPOSURES	WHY IT MATTERS
Cyber insurance conditions have been comparatively stable, but underwriting remains disciplined.	BEC, phishing, help desk impersonation, account takeover and AI-enabled social engineering.	Strong controls can reduce loss potential and may influence cyber insurance availability, terms and pricing.

WHAT IS CHANGING

The cyber insurance market entered 2026 with greater pricing stability and expanded capacity after several years of volatility. The source newsletter notes that well-managed organizations may continue to see favorable renewal conditions, while accounts with weaker controls or poor loss history can face a very different underwriting response.

At the same time, the threat environment continues to evolve. Artificial intelligence can help malicious actors move faster, while business email compromise, phishing, impersonation and account takeover remain practical threats to organizations of every size. The FBI describes today's digital environment as a larger-than-ever attack surface and continues to emphasize cyber resilience and rapid reporting.

WHAT IT MEANS FOR YOUR BUSINESS

Cyber insurance should not be viewed separately from the controls used to protect the business. Underwriters increasingly want evidence that safeguards are implemented, maintained and tested. The goal is not simply to complete an application; it is to build a system that reduces the likelihood and impact of an incident.

KEY POINT

Cyber insurance can help finance a loss, but it does not replace prevention. Strong authentication, secure email, protected backups, tested response plans and team-member awareness work together to strengthen cyber resilience.

Protect Team Members. Control Risk. Control the Cost of Risk.

THE HOLT GROUP LLC | www.theholtgroupllc.com

REGULATORY UPDATE

Working Together. Evolving Together.

The Holt Group

Cyber Risk in 2026: Strong Controls Matter More than Ever

Evolving Threats, Social Engineering and Underwriting Expectations are Keeping Cyber Resilience in Focus

SOCIAL ENGINEERING REMAINS A HUMAN AND TECHNOLOGY RISK

The source newsletter highlights tech-support scams, help-desk impersonation and business email compromise as recurring exposures. These attacks often create urgency, impersonate a trusted person or service, and attempt to persuade a team member to provide credentials, approve access, change payment information or transfer funds. The FBI continues to identify business email compromise as one of the most financially damaging online crimes. Its current guidance recommends examining email addresses and URLs carefully, using multi-factor authentication, and independently verifying payment requests and changes to account or payment information.

CONTROLS TO REVIEW

- Authentication - use strong multi-factor authentication and prioritize phishing-resistant methods for high-impact accounts where practical.
- Email Protection - use SPF, DKIM and DMARC, malicious-content filtering, and controls that help identify suspicious messages.
- Payment Verification - independently verify wire transfers, vendor bank-account changes and unusual payment requests using a known contact method.
- Endpoint And Vulnerability Protection - maintain security software, patch systems, monitor endpoints and address known vulnerabilities on a risk-based schedule.
- Backups And Recovery - maintain protected backups and confirm that critical systems and data can be restored.
- Incident response - maintain a written response plan, identify outside resources in advance and periodically test the process.
- Team-Member Education - train people to recognize urgency, impersonation, suspicious support requests and attempts to bypass normal procedures.

WHAT TO KNOW

Technology alone cannot stop every social-engineering loss. A strong control environment combines technical safeguards with clear procedures, independent verification and team members who know when to stop and ask questions.

Protect Team Members. Control Risk. Control the Cost of Risk.

THE HOLT GROUP LLC | www.theholtgroupllc.com

REGULATORY UPDATE

Working Together. Evolving Together.

The Holt Group

Cyber Risk in 2026: Strong Controls Matter More than Ever

Evolving Threats, Social Engineering and Underwriting Expectations are Keeping Cyber Resilience in Focus

IF A FINANCIAL FRAUD OCCURS

Act quickly. The FBI advises organizations affected by business email compromise or other cyber-enabled financial fraud to contact their financial institution immediately and report the incident to the FBI's Internet Crime Complaint Center (IC3). Rapid reporting may improve the opportunity to freeze or recover funds.

NEXT STEPS

- Review the cyber controls represented on insurance applications and confirm they match actual practices.
- Identify the systems, accounts, vendors and payment processes that could create the greatest operational or financial disruption.
- Test payment-change and wire-transfer verification procedures with leadership, finance and accounting personnel.
- Review access privileges and strengthen authentication for administrators, executives and other high-impact accounts.
- Confirm backups and incident-response procedures are documented, protected and periodically tested.
- Provide recurring team-member education using realistic examples of phishing, BEC, help-desk impersonation and urgent payment requests.
- Review cyber insurance limits, sublimits, retentions and social-engineering coverage as part of the broader Risk Finance Plan.

THE HOLT GROUP PERSPECTIVE

Cyber risk is not simply an information-technology issue or an insurance issue. It is an operational risk that connects technology, people, procedures, leadership and risk finance. The strongest approach is to understand where the business is vulnerable, build practical controls around those exposures, train team members to recognize suspicious activity, and use insurance as one part of a broader plan for resilience and recovery.

Protect Team Members. Control Risk. Control the Cost of Risk.

THE HOLT GROUP LLC | www.theholtgroupllc.com

REGULATORY UPDATE

Working Together. Evolving Together.

The Holt Group

Cyber Risk in 2026: Strong Controls Matter More than Ever

Evolving Threats, Social Engineering and Underwriting Expectations are Keeping Cyber Resilience in Focus

LEADERSHIP NOTE

A favorable cyber insurance market can create opportunities to evaluate limits, retentions and coverage. It should not create complacency. Threats can change quickly, and underwriting outcomes continue to depend heavily on the organization's control environment and loss history.

SOURCES

- Zywave, Cyber Risks & Liabilities Newsletter - Q1 2026.
- Federal Bureau of Investigation (FBI), Cyber; Business Email Compromise; Improve Cyber Resiliency, accessed October 2026.
- Federal Bureau of Investigation, 2025 Internet Crime Report release, April 6, 2026.



RISK MANAGEMENT
UNIVERSITY

COMPLIANCE

RISK PREVENTION

RISK FINANCE

COMMUNICATION

Protect Team Members. Control Risk. Control the Cost of Risk.

THE HOLT GROUP LLC | www.theholtgroupllc.com

This Regulatory Update is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for appropriate advice. © Zywave, Inc., The Holt Group LLC All rights reserved. All images are from Google Images and Story Blocks. **Revised 2027**