Operational Alpha:
Building Cyber Resiliency in Private Markets

MAY 08, 2026

AKRAM
Assurance, Advisory & Tax

Linedata

CONDUIT

OFFICIALLY REGISTERED

AKRAM & ASSOCIATES is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Program level : Basic

No prerequisites are required

No advance preparation is required

AKRAM
Assurance, Advisory & Tax

Linedata

CONDUIT

M

For more information please contact:

Muhammad A. Akram - CPA and Founding Member Toll-Free: 844-386-3829 | makram@aifundservices.com

FEATURED PANELISTS

Moderator

Anna Miller
Strategic Growth Advisor
Akram & Associates PLLC

Hameed
CISO
Akram & Associates PLLC

Brian Long
SVP & Global Head of Sales
Linedata

Dave Adams
COO & Co-Founder
Conduit Security

Matt Stevens
Senior Risk Advisor
Marsh

About

Akram is a trusted adviser to alternative fund managers – the cornerstone of our business. Our laser focus on this industry allows us to provide highly specialized accounting, audit, and tax services that are accurate and affordable. Our team of professionals is well versed in the nuances of hedge fund, private equity fund, venture capital fund, CTA , digital asset fund, real estate fund, and family office entity structures and strategies, positioning Akram as an expert resource to both emerging managers and sophisticated managers overseeing multiple funds.

With 25+ years of experience and 700 clients in 50 countries, Linedata's 1100 employees in 20+ offices provide global humanized technology solutions and services for the asset management and credit industries, helping its clients evolve and operate at the highest levels.

Conduit's SaaS tool defends investment managers against wire fraud. Our clients include the most sophisticated managers and companies in the world. We have protected billions and our clients have never lost a dollar to wire fraud.

Marsh Risk is a part of Marsh. Together with Mercer, Guy Carpenter, and Oliver Wyman, we help organizations build resilience and competitive advantages from every angle. With annual revenue over $24 billion and more than 90,000 colleagues in 130 countries, Marsh helps build the confidence to thrive through the power of perspective.

Agenda

- Current Cyber Threat Landscape
- Expanded Threat Due to AI
- Operational Resiliency Framework
- Financial & Alternative Fund Industry Implications
- Firm-Size Checklists & Universal Controls
- Your Next 90 Days
- Q&A / Discussion

Current Cyber Threat Landscape

The attack surface has never been larger.

BUSINESS IMPACT

Impact on Your Organization

Operations Halted
Systems offline · 21 days avg downtime · Supply chain disrupted

Data Loss
Customer records exposed · IP stolen · Regulatory breach triggered

Financial Damage
Ransom demands · Recovery costs · Lost revenue · Regulatory fines

Reputation Harm
Customer trust eroded · Negative media · Partner confidence lost

Legal & Compliance
GDPR · SEC disclosure obligations · Regulatory investigations

BY THE NUMBERS – The Threat is Real

70%

Of organizations experienced at least 1 material third party cyber incident in the past year

88%

Of organizations are concerned about supply chain cybersecurity risks

30%

Of breaches are linked to third party involvement (twice as much as last year)

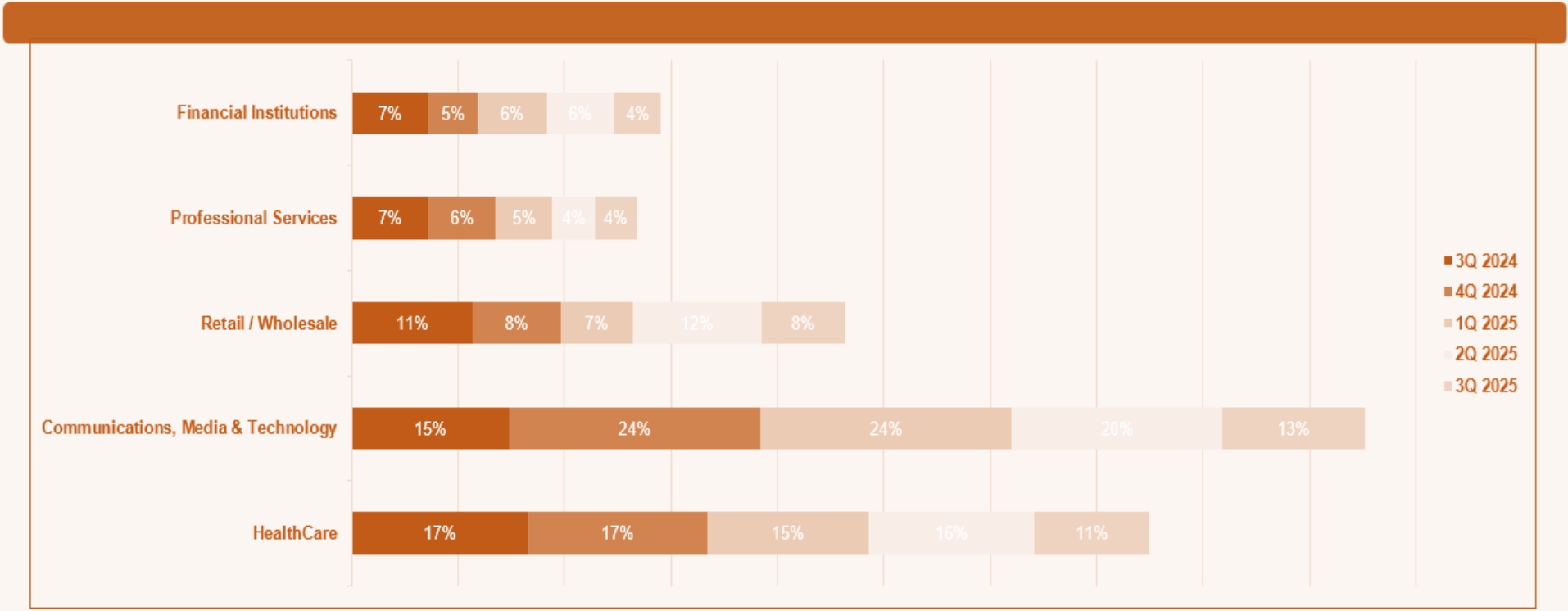
<50%

Of organizations monitor cybersecurity across even 50% of their supply chain

26%

Of organizations include incident response in their supply chain cybersecurity programs

BY THE NUMBERS – Top Five Affected Industries



The Communication, Media and Technology sector has seen an increase in frequency compared to other sectors for quarters.

POLLING QUESTION

How would you describe your current cybersecurity resilience approach?

a) Proactive and well-integrated

b) Defined but siloed across teams/providers

c) Reactive / incident-driven

d) Still developing

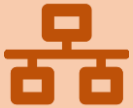
TOP ATTACK VECTORS – Where Threats Enter

Phishing & Social Eng.

Ransomware

Data Exfiltration

Cloud Misconfiguration



Supply Chain Attacks

Zero-Day Exploits

POLLING QUESTION

Where does your organization feel most exposed today?

a) Phishing / social engineering

b) Ransomware / malware

c) Third-party / vendor risk

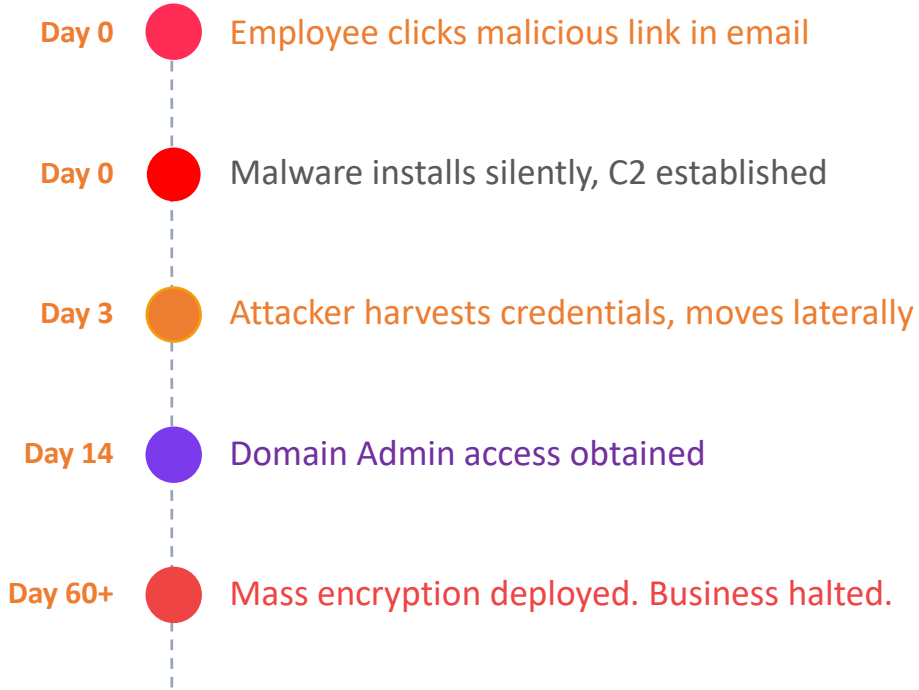
d) Insider risk (intentional or accidental)

What is an Attack Really Like?

From first click to full compromise.

REAL ATTACK SCENARIO

One Phishing Email → Full Breach



POLLING QUESTION

If a cyber incident occurred, how confident are you in your ability to recover quickly?

a) Very confident (tested plan in place)

b) Somewhat confident (plan exists, limited testing)

c) Not confident (plan is incomplete or untested)

d) Unsure

Expanded Threat Due to AI

AI doesn't just defend — it also attacks.

HOW AI CHANGES THE GAME

AI-Powered Threats

Hyper-Personalized Phishing

AI crafts convincing spear-phishing at massive scale

Deepfake Social Engineering

Cloned voices & video to impersonate executives

Automated Exploitation

AI finds and attacks vulnerabilities in real-time

AI-Powered Malware

Self-modifying code that evades traditional detection

Operational Resiliency

Prepare. Detect. Respond. Recover.

COMPLIANCE DEADLINE AUM <1B: JUNE 3, 2026

Best Practices to Prepare for Reg S-P

01 Governance & Accountability

- Named program owner with documented authority
- Leadership briefed on amended rule obligations
- Written information security program in place
- Annual policy review & privacy notice delivery

02 Customer Info Mapping

- Inventory of all systems storing customer data
- Physical, cloud & endpoint locations documented
- Data flows mapped across internal & third parties
- Classification scheme with handling rules

03 Detection & Monitoring

- Technical controls to detect unauthorized access
- Logging enabled on all critical systems
- Logs actively monitored with escalation paths
- Documented 'reasonably likely' methodology

04 Incident Response Program

- Written IRP covering detection through recovery
- Legal & compliance integrated from the outset
- Explicit notification decision criteria defined
- Annual tabletop exercises with documented results

05 Customer Notification

- Written 30-day notification procedures
- Ability to identify specific affected customers
- Pre-approved notification templates prepared
- Parallel state & regulatory obligations mapped

06 Vendor Oversight

- Inventory of all third parties touching customer data
- Contracts require written safeguards
- 48–72 hr vendor incident notification SLA
- Documented due diligence & reassessment cadence

07 Safeguards & Controls

- Role-based access controls with periodic reviews
- MFA enforced on all remote & customer-data access
- Encryption at rest and in transit
- Written secure disposal for physical & electronic records

08 Documentation & Recordkeeping

- All incidents documented — including non-notifiable
- Decision rationale recorded for notify/don't-notify
- Log & artifact retention aligned to exam obligations
- Examination-ready evidence binder organized0

09 Testing & Continuous Improvement

- Annual tabletops with full response team
- Annual security & customer-data handling training
- Key controls validated on defined cadence
- Periodic third-party program assessment

POLLING QUESTION

What is your biggest concern over the next 12 months?

a) AI-driven attacks (phishing, deepfakes, automation)

b) Increasing sophistication of ransomware

c) Third-party / vendor vulnerabilities

d) Regulatory / compliance expectations

e) Keeping up with internal resources / bandwidth

THE RESILIENCE FRAMEWORK

Four Pillars of Cyber Resilience

01

Prepare

Risk assessment · Zero Trust · Security training

02

Detect

SIEM · XDR · Threat intel feeds

03

Respond

IR playbooks · Isolation · Communication plan

04

Recover

Backups · RTO/RPO goals · Post-incident review

ARE YOU READY?

Resiliency Readiness Check

- ✓ Do you have a tested incident response plan?
- ✓ Are backups isolated and tested regularly?
- ✓ Is MFA enforced across all privileged accounts?
- ✗ Can you detect a breach within 24 hours?
- ✗ Do employees receive regular security training?
- ✗ Is your supply chain security assessed annually?

NEXT STEPS

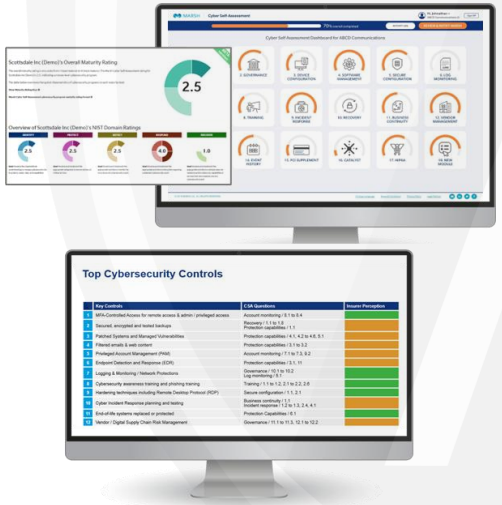
How Akram & Their Partners Can Help

1) **Marsh**: Take the Cyber Self-Assessment | Marsh - Reference AKRAM webinar w/ matt.stevens@marsh.com

2) **Akram**: Take a brief Reg S-P Assessment Survey to identify your compliance gaps and receive personalized recommendation of services from Hameed

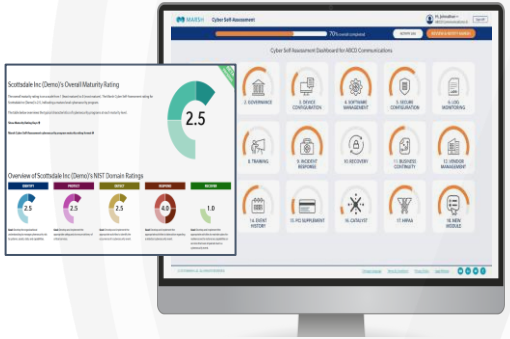
3) **Conduit**: Solve Wire Fraud: Conduit SaaS tool Validates Payments: www.conduitsecurity.com

4) **Linedata**: Download the Regulation S-P Compliance Readiness Questionnaire here:



Cyber Self-Assessment

Digital diagnostic tool to enable better analysis, insights, advice, and transactional capabilities



Benefits:

- **Cyber Insurance application**: responses become an application document
- **Cybersecurity Scorecard**: with commentary based on NIST framework
- **Top Cybersecurity Controls report**: heat map of controls influencing insurability
- **Controls benchmarking**: Cybersecurity position compared to peers
- **Cyber risk analytics**: More robust loss modeling

Features:

- **Collaboration tool**: Multiple participants can contribute to the same form simultaneously. Activity Log tracks changes.
- **Ease of updates**: Last year's responses automatically prefill this year's form for update – any new questions will be flagged.
- **Easy to use**: Ability to save progress and add commentary if needed.
- **Data security**: Access is controlled and login requires multi-factor authentication. Responses are encrypted and securely stored.
- **Coverage sections**: Includes Tech E&O, Cyber, Operational Technology, and Media questions

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Evaluate your cybersecurity maturity and prepare for insurance marketing by completing Marsh's Cyber Self-Assessment.
2. Use Marsh Cybersecurity Marketplace Services for access to a curated portfolio of cybersecurity vendor solutions and holistic vendor procurement support.

- Multifactor authentication for remote access and admin/privileged controls
- Endpoint Detection and Response (EDR)
- Secured, encrypted, and tested backups
- Privileged Access Management (PAM)
- Email filtering and web security
- Patch management and vulnerability management
- Cyber incident response planning and testing
- Cybersecurity awareness training and phishing testing
- Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
- Logging and monitoring/network protections
- End-of-life systems replaced or protected
- Vendor/digital supply chain risk management

Note: *Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class*

Claims & Incident Management

How you respond makes all the difference

Prepare

Creating and testing IR plans reduces losses by $1.49 M on average – IBM Cost of a Data Breach Report 2023

- Marsh Central
- Incident response plan review and development
- Incident response vendor selection

Test

Well-practiced teams know their roles, responding quickly and effectively.

- Tabletop exercises & crisis simulations

Respond

A coordinated, holistic effort is vital for effective incident response.

- Marsh Central
- Active Incident Response (AIR) support

Recover

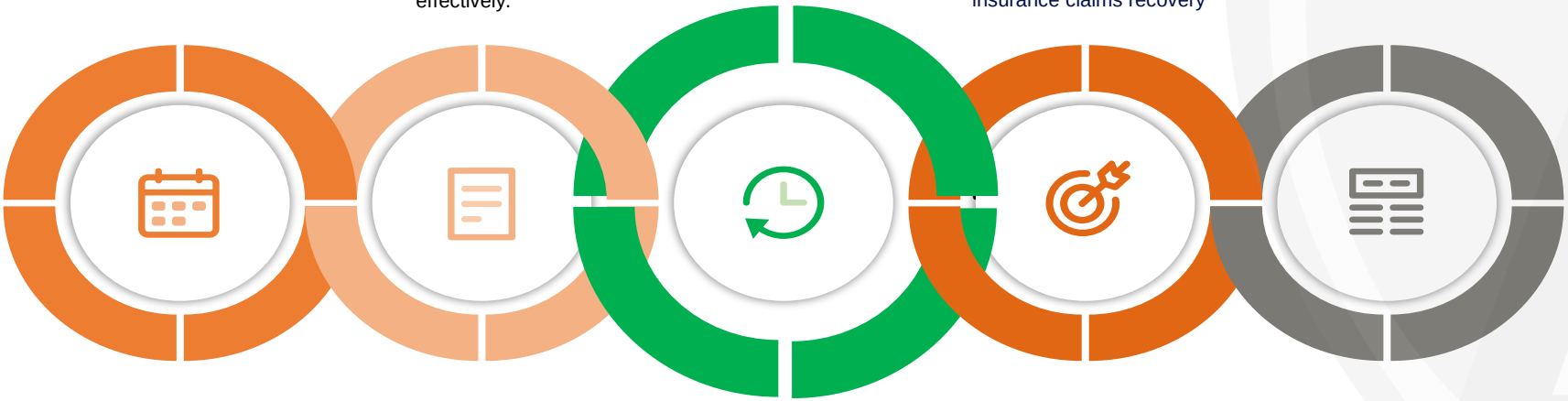
Expert support ensures proactive navigation of cyber claims complexity, maximizing insurance claims recovery

- Claims preparation/ forensics accounting
- Claims advocacy

Enhance

Convert learnings and challenges into opportunities for growth

- Resilience Roadmap Development




Security is not a product.
It's a process.
Stay informed. Stay prepared. Stay resilient.

THANKS FOR LISTENING

AKRAM Assurance, Advisory & Tax | Linedata | CONDUIT | M

For more information please contact:

Muhammad A. Akram - CPA and Founding Member Toll-Free: 844-386-3829 | makram@aifundservices.com