



THE STATE OF CYBERSECURITY 2026

THE (OVER) CONFIDENCE GAP

Emerging threats and trends in financial services, healthcare, technology, manufacturing and retail

EXECUTIVE SUMMARY

TWELVE MONTHS LATER, THE GAP HAS WIDENED

Last year we reported that financial services firms were facing an unprecedented level of cyber risk. A year later the numbers have moved the wrong way, and the pressure has spread well beyond banks and investment firms.

The average cost of a U.S. data breach reached \$11.5 million in 2026, up from \$10.22 million the year before, according to IBM. One in four malicious breaches IBM studied was AI-enabled. And Verizon found that nearly half of the breaches involved a third party, up from 30% a year earlier.

Despite this, most leaders still say they feel ready. In Beazley’s 2026 global survey of 3,500 business leaders, 82% said they were prepared for cyber risk and 78% said they could fully recover financially from an attack. Yet U.S. breach costs set another record, and the average breach took 247 days to find and contain.

That distance between confidence and reality is the subject of this report.

We look at what changed this year in the cyber threat landscape, which regulations now apply, how the picture differs across the industries we serve, and where leadership teams can make real progress in the year ahead.

CONFIDENCE

82%

of business leaders say they are prepared for cyber risk

78%

say they could fully recover financially from an attack

Beazley Risk & Resilience 2026

REALITY

\$11.5M

average cost of a U.S. data breach, another record

247 days

on average to find and contain a breach

IBM Cost of a Data Breach Report 2026

KEY FIGURES

\$11.5M

Average cost of a U.S. data breach

IBM Cost of a Data Breach Report 2026

1 in 4

Malicious breaches that were AI-enabled

IBM Cost of a Data Breach Report 2026

48%

Breaches that involved a third party

Verizon 2026 DBIR

73%

Ransomware victims that were mid-market companies

Black Kite 2026 Mid-Market Report

82%

Business leaders worldwide who say they are prepared for cyber risk

Beazley Risk & Resilience 2026

IN THIS REPORT

YEAR IN REVIEW	04
THE MID-MARKET IS THE TARGET	06
REGULATORY UPDATE	08
INDUSTRY SNAPSHOTS	10
PRIVATE EQUITY	11
WHERE TO ACT	15
HOW WE CAN HELP	19

YEAR IN REVIEW

WHAT CHANGED SINCE OUR LAST REPORT

MEASURE	2025 EDITION	THIS YEAR
Average U.S. breach cost (IBM)	\$10.22M	\$11.5M
Average global breach cost (IBM)	\$4.88M	\$4.99M
Average financial sector breach cost (IBM)	\$5.56M	\$6.29M
Breaches involving a third party (Verizon)	30%	48%
Breaches involving the human element (Verizon)*	68%	62%

*2025 edition figures are from IBM’s 2024 report and Verizon’s 2024 DBIR, except U.S. and financial sector breach costs (IBM 2025) and third-party share (Verizon 2025). Verizon has changed how it defines the human element, so the two figures are not strictly comparable.

1 in 4

malicious breaches were AI-enabled, a 56% increase (IBM 2026)

AI MOVED FROM EXPERIMENT TO ATTACK TOOL

IBM found one in four malicious breaches was AI-enabled this year, a 56% increase, driven mostly by deepfake impersonations and AI-generated malware. Those breaches cost about \$1 million more than average.

30% **48%**

breaches involving a third party, last edition vs. this year (Verizon)

THIRD-PARTY BREACHES REACHED A NEW HIGH

Vendor risk has been a priority for years, but the problem is still growing: third-party involvement breaches rose from 30% to 48% in a single year from Verizon data. Several of the largest incidents it studied hit multiple vendors in the same campaign.

247

days on average to identify and contain a breach, the first increase in five years (IBM 2026)

RESPONSE GOT SLOWER

The average time to identify and contain a breach rose to 247 days, the first increase in five years. IBM links the increase to more complex AI-driven and multi-vector attacks, and breaches involving data stores in multiple locations took the longest, at 256 days. But organizations that used AI and automation extensively in security operations cut breach costs by \$1.93 million and identified and contained breaches 65 days faster than organizations that did not use these tools.

WHAT WORKS: AI AND AUTOMATION IN SECURITY OPERATIONS

\$1.93M

lower breach costs for organizations that used these tools extensively

65 days

faster to identify and contain a breach

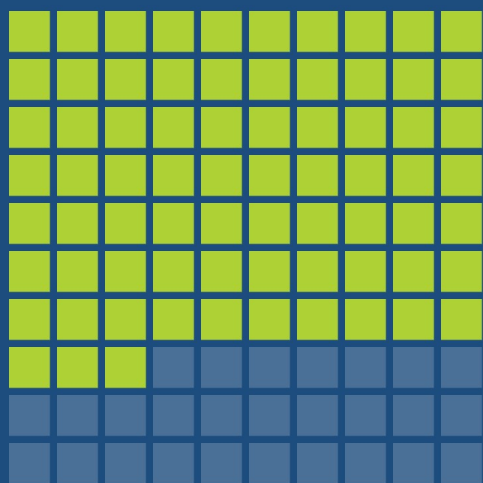
256 days

for breaches involving data stores in multiple locations, the longest of all

IBM Cost of a Data Breach Report 2026

THE MID-MARKET IS THE TARGET

LARGE ENTERPRISES GARNER HEADLINES. MOST ATTACKS HIT THE MID-MARKET



73%

of ransomware victims were mid-market companies with \$10 million to \$1 billion in annual revenue

Black Kite 2026, analysis of 13,336 ransomware incidents, January 2023 through June 2026

Most breach reporting focuses on Fortune 500 companies and billion-dollar incidents. The reality on the ground is different. Black Kite's 2026 analysis of 13,336 ransomware incidents from January 2023 through June 2026 found that 73% of victims were mid-market companies with \$10 million to \$1 billion in annual revenue. The lower mid-market, companies with \$10 million to \$50 million in annual revenue, made up the largest share at 54% of all mid-market victims.

The volume is climbing. Ransomware incidents against mid-market firms rose 44% between 2023 and 2025, from 2,320 to 3,340 incidents per year. But the proportion held steady at roughly three in four, meaning mid-market companies are not getting caught in crossfire meant for larger targets. They are the target. Ransomware is also a large share of the overall problem: Verizon found it in 48% of all breaches this year, up from 44% of the year before.

Coveware's incident data tells the same story from a different angle: mid-sized organizations with 11 to 1,000 employees made up 64% of ransomware victims in Q2 2025. These companies are large enough to offer attackers a meaningful payout, but they may lack the security resources of larger enterprises.

MID-MARKET RANSOMWARE INCIDENTS PER YEAR



Black Kite 2026

+44%

rise in mid-market ransomware incidents between 2023 and 2025, while the share held steady at roughly three in four

\$200K to \$800K

a breach in this range can threaten a mid-market business itself

WHAT GLOBAL AVERAGES MISS

For companies in this range, the IBM global averages understate the problem in one way and overstate it in another. A \$4.99 million global average includes organizations with resources to absorb the hit. In our experience working with mid-market clients, a breach in the \$200,000 to \$800,000 range can threaten the business itself, especially when you add lost contracts, customer churn, and regulatory consequences that unfold over months.

KEY FIGURES

METRIC	FIGURE	SOURCE
Ransomware victims that were mid-market companies	73%	Black Kite 2026 (13,336 incidents)
Lower mid-market share (\$10M-\$50M revenue)	54%	Black Kite 2026
Mid-sized companies (11-1,000 employees) as share of ransomware victims	64%	Coveware Q2 2025
Increase in mid-market ransomware incidents, 2023 to 2025	44%	Black Kite 2026
Average breach cost for companies under 500 employees	\$3.31M	IBM 2023

REGULATORY UPDATE

THE REGULATIONS CAUGHT UP WITH THE RISK

Last year’s report flagged several changes on the horizon. Most have now arrived, and they share a theme: regulators increasingly expect a written, tested incident response program and documented oversight of vendors.

INVESTMENT FIRMS

SEC REGULATION S-P IS NOW IN EFFECT FOR ALL COVERED FIRMS

Dec 3, 2025

Compliance deadline for larger firms

Larger firms had to comply by December 3, 2025, and smaller firms by June 3, 2026. The amended rule requires a written incident response program and notice to affected individuals within 30 days of learning that their sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Firms must also oversee their service providers, who are required to notify the firm within 72 hours of becoming aware of a breach of a customer information system they maintain.

Jun 3, 2026

Compliance deadline for smaller firms

30 days

to notify affected individuals

The SEC named Regulation S-P compliance an examination priority for fiscal year 2026.

72 hours

for service providers to notify the firm

BEFORE YOUR NEXT EXAM

Firms that have not yet tested their incident response program against the 30-day notice clock or confirmed that their service providers can meet the 72-hour deadline should do so before their next exam.

Retired

The FFIEC Cybersecurity Assessment Tool was sunset after August 2025

BANKING

THE FFIEC CYBERSECURITY ASSESSMENT TOOL HAS BEEN RETIRED

The FFIEC sunset its Cybersecurity Assessment Tool after August 2025 and pointed institutions to newer frameworks, including NIST Cybersecurity Framework 2.0, the CRI Profile 2.0, and CISA's Cybersecurity Performance Goals. Institutions that have not yet mapped their program to one of these other frameworks should make it a 2027 priority.

July 2027

Projected final action on the HIPAA Security Rule rewrite, per the federal regulatory agenda

HEALTHCARE

THE HIPAA SECURITY RULE OVERHAUL IS DELAYED, NOT DROPPED

HHS proposed the first major rewrite of the Security Rule in January 2025. The federal regulatory agenda now projects final action in July 2027. The current rule remains fully enforceable, and many of the proposed controls, such as asset inventories, encryption, and multifactor authentication, can be built now, before the overhaul happens.

63%

of breached organizations had no policy to manage AI or detect unapproved AI use (IBM 2025)

ALL INDUSTRIES

AI GOVERNANCE IS STILL VOLUNTARY, AND STILL RARE

No single U.S. framework governs AI security yet. In IBM's 2025 breach study, 63% of breached organizations had no policy to manage AI or detect unapproved AI use, even as AI tools spread across their operations. Until a framework arrives, organizations should set their own AI use policy and keep an inventory of the AI tools employees are using.

INDUSTRY SNAPSHOTS

SAME THREATS, DIFFERENT PRESSURE POINTS

The threats in this report touch every sector, but each industry feels them differently. Here is where we've seen the most pressure among the organizations we work with.

FINANCIAL SERVICES

\$6.29M

Average financial sector breach cost, up from \$5.56M (IBM 2026)

Finance and insurance were the second most attacked sectors for the fifth year in a row in IBM's X-Force's Threat Intelligence Index, accounting for 27% of incidents. With Regulation S-P now fully in effect, examiners will expect investment firms to show that their incident response plans and vendor oversight programs work in practice.

WHAT TO PLAN FOR & TEST

- Deepfake impersonation of executives in payment and wire approvals
- Breaches that start at a payment processor, core provider, or cloud vendor
- Testing incident response against the 30-day and 72-hour notice clocks

HEALTHCARE

\$6.64M

Average healthcare breach cost, the highest of any industry for the 13th year (IBM 2026)

Healthcare breaches remain the most expensive of any industry. While the HIPAA Security Rule rewrite is delayed, enforcement under the current rule continues, and inadequate risk analysis remains one of the most commonly cited deficiencies in OCR investigations.

WHAT TO PLAN FOR & TEST

- An enterprise-wide risk analysis that is current and documented
- Business associates with access to patient data
- Legacy and connected medical systems that cannot be patched quickly

PRIVATE EQUITY

CYBER RISK IS NOW DEAL RISK

Portfolio companies carry the same exposure with less oversight

94%

of PE firms suffered some financial impact from cybersecurity risk

Kroll 2026, survey of 325 portfolio leaders

\$2.1M

average financial impact per incident

Kroll 2026

1 in 2

PE portfolio companies face elevated or high cybersecurity risk

ACA Group 2026, 300+ portfolio companies

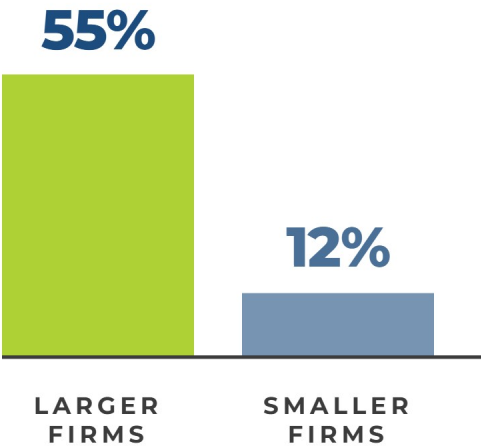
Private equity firms buy, grow, and sell businesses, and cyber risk now touches every stage of that cycle. Kroll's 2026 global survey of 325 portfolio leaders found that 94% of PE firms suffered some financial impact from cybersecurity risk, averaging \$2.1 million in financial impact per incident.

ACA Group's 2026 benchmarking report, drawing on assessments of more than 300 portfolio companies across 18 industries and 12 countries, found that half of PE portfolio companies face elevated or high cybersecurity risk. The characteristics that make a company attractive to private capital, including rapid growth, operational complexity, and speed of execution, also increase the number of risk points that attackers can exploit.

Cybersecurity goes beyond compliance. It can help protect intellectual property and trade secrets at the core of the investment thesis.

THE GOVERNANCE GAP

PE firms that govern cybersecurity risk through a formal mandate to portfolio company managers



Kroll 2026

The governance gap is wide. Kroll found that 55% of larger PE firms govern cybersecurity risk through a formal mandate to portfolio company managers, compared to just 12% of smaller firms. Yet 96% of PE firms expect the importance of portfolio cybersecurity to increase over the next 12 months.

The risk does not stay contained. A single vulnerable portfolio company can become an entry point into vendors, customers, or other companies using shared platforms and limited partners (LPs) increasingly know this. Institutional investors, pensions, and sovereign wealth funds are no longer treating cyber risk as an individual portfolio company’s problem. Funds that lack an adequate cyber plan across their portfolio are at a disadvantage, because cybersecurity goes beyond compliance. It can help protect intellectual property and trade secrets at the core of the investment thesis.

WHAT PE FIRMS SHOULD BE DOING

01

PRE-ACQUISITION

Cyber due diligence needs to go beyond a checkbox exercise. Inherited risk that is not priced in at close can become a liability during the hold period.

02

DURING THE HOLD PERIOD

Funds should establish a portfolio-wide baseline for cybersecurity. A fund needs to be able to see where risk is concentrated across portfolio companies and move from allowing each company to manage systemic risk independently.

03

AT EXIT

Demonstrate that the company’s cybersecurity posture improved under your ownership. Buyers and their advisers are increasingly incorporating cyber risk into their valuations.

MANUFACTURING & DISTRIBUTION

27.7%

Share of incidents, making manufacturing the most attacked industry for the fifth year (IBM X-Force 2026)

Downtime is the attacker's leverage. Exploitation of public-facing applications was the most common way in, at 32% of manufacturing incidents IBM responded to, and connected plant systems widen the target. Manufacturing also leads the mid-market ransomware count: Black Kite found it accounted for more than a quarter of all mid-market victims, more than the next two sectors combined. The convergence of IT and operational technology networks means a ransomware attack that starts in a corporate email inbox can reach the factory floor.

WHAT TO PLAN FOR & TEST

- Ransomware that halts production or shipping
- Remote access used by suppliers and equipment vendors
- Separation between office IT and operational technology

TECHNOLOGY

21%

Breached organizations with an incident involving an AI model or application, up from 13% a year earlier (IBM 2026)

AI systems are now a breach category of their own. As organizations rush to deploy AI tools, they are creating new attack surfaces: models that process sensitive data, training pipelines that can be poisoned, and AI agents with broad system access. IBM also found that fewer than half of organizations are actively securing the non-human identities that power their AI workflows, leaving AI models, training data, and AI agents exposed to exploitation.

WHAT TO PLAN FOR & TEST

- Unapproved AI tools handling customer or proprietary data
- Non-human identities powering AI workflows that hold broad access with little or no monitoring
- AI models trained on or processing sensitive customer, patient or proprietary data without governance controls

RETAIL

\$402M*

Estimated hit to operating profit at Marks & Spencer after its April 2025 attack

One of the year's most widely reported retail breaches started with a phone call. Attackers reportedly posed as employees to get an IT help desk to reset credentials, then deployed ransomware. The U.K. retailer paused online orders for weeks.

HOW THE ATTACK UNFOLDED

01

Attackers reportedly posed as employees on a phone call

02

The IT help desk reset their credentials

03

They deployed ransomware, and online orders paused for weeks

WHAT TO PLAN FOR & TEST

- Identity checks at the help desk before any password or MFA reset
- Outsourced IT and service desk providers
- Seasonal staff and store systems with shared logins

*Marks & Spencer estimated a £300 million hit to group operating profit in May 2025, about \$402 million at both the May 2025 and current exchange rates.

WHERE TO ACT

FIVE PRIORITIES FOR THE YEAR AHEAD

01

PUT (OR KEEP) CYBER RISK AT THE TOP OF THE LEADERSHIP AGENDA

Many of the incidents in this report were failures of oversight, more than they were failures of technology. This matters to regulators and it's part of how financial liability is determined during breach-related litigation. Why? Because every company has unremediated vulnerabilities. Demonstrating that there's an understanding of risk and there's a properly prioritized plan mitigates regulatory and financial liability. Boards and executive teams own cyber risk the way they own financial risk, including establishing clear policies on how employees may use AI tools and ensuring effective controls are in place.

A quantified risk assessment is the gold standard. Measuring the cost of risk gives leadership a dollar figure to work with, not just a color on a heat map. When the board can see what a breach actually costs in their environment, with their data, the conversation shifts from "Are we compliant?" to "Are we protected?" and the company knows how to prioritize remediation efforts. For PE-backed companies, that assessment should happen at acquisition and at regular intervals during the hold period, not just when a regulator or buyer asks.

QUESTIONS FOR YOUR LEADERSHIP TEAM

- Can we quantify the cost of cyber risk?
- Do we have a documented, prioritized risk plan and do we track progress over time?
- Who reports cyber risk to the board, and how often?
- Do we have an approved AI use policy, and can we tell when it is ignored?
- **For PE firms:** Can you see where cyber risk is concentrated across your portfolio, do you require portfolio companies to conduct regular assessments, and do you monitor their remediation efforts?

02 IDENTITY REMAINS THE NEW PERIMETER

Attackers increasingly log in rather than break in. Zero Trust, the approach to identity management where no user, device, or request is trusted by default, even inside a company's own network, verifies every user, device, and request, limits access to only what each role needs and extends the same discipline to service accounts and AI agents. For mid-market companies without a dedicated security operations center, identity controls are the highest-leverage investment available.

QUESTIONS FOR YOUR LEADERSHIP TEAM

- Could someone talk our help desk into resetting a password or MFA device?
- Which accounts, human or not, hold standing administrator access?
- Do we have a plan to move beyond static passwords and multifactor authentication towards more foolproof access controls like biometrics and other phishing-resistant credentials?

03 REHEARSE YOUR INCIDENT RESPONSE BEFORE YOU NEED IT

Organizations that find breaches themselves and use automation to triage and execute predefined containment steps typically face substantially smaller financial consequences than those that learn of a breach from the attacker. Mid-market companies are particularly vulnerable here: many have a plan on paper but have never conducted a tabletop exercise to test it under conditions that simulate real pressure, real time constraints, and real coordination across legal, IT/IT security, and leadership. If the company has outside counsel or an incident response firm on retainer, they should be included in these rehearsals.

QUESTIONS FOR YOUR LEADERSHIP TEAM

- When did we last run a tabletop exercise with executives in the room?
- Can we meet a 30-day customer notification deadline with our current process?

04 SECURE AI AND CLOUD ADOPTION AS IT HAPPENS

AI tools and cloud services are finding their way into companies' environments faster than security teams can review them. Keep an inventory of the AI tools and applications in use, apply access controls to the models and data behind them, and test continuously rather than once a year.

QUESTIONS FOR YOUR LEADERSHIP TEAM

- Which AI tools and applications are employees using today, and do we know which are approved?
- When was our environment last tested by working with offensive security experts to try to break in?

05 KNOW WHAT YOUR VENDORS CAN REACH

Nearly half of the breaches involve a third party, and a gap in a vendor's security can become a breach in your environment. That makes vendor risk management a critical part of your own security program. The more of your data a vendor can reach, the more scrutiny it should get, from contract terms and SOC reports to regular access reviews. For mid-market companies that rely heavily on outsourced IT, managed services, and cloud providers, this is not optional. Your vendor's weakness is your weakness.

QUESTIONS FOR YOUR LEADERSHIP TEAM

- Which vendors can access or store our most sensitive data, and when did we last review their security posture?
- Do our contracts require prompt notice when a vendor is breached?
- **For PE firms:** Do your portfolio companies share vendors, and do you have visibility into that overlap?

YOUR VENDOR'S WEAKNESS IS YOUR WEAKNESS.

48%
of breaches involved a third party



The over-confidence gap is real. I saw it play out over and over during my years investigating cyber intrusions for the FBI. The organizations that got hit the hardest were rarely the ones that thought they were vulnerable. They were the ones who were certain they were covered. They had firewalls, they had policies on paper, and they had passed their last audit. What they did not have was someone who had tested whether any of it actually worked under pressure. The attacker was the first real test, and by then it was too late. **Confidence without evidence is just exposure you haven't measured yet.**"



KORY PATRICK, CISSP
CYBERSECURITY PRACTICE LEADER
PRINCIPAL, RISK ADVISORY SERVICES

CONCLUSION

CLOSING THE (OVER)CONFIDENCE GAP

Confidence is useful when it's anchored in evidence: knowing where sensitive data lives and who, or what, can reach it, and practicing response to multiple intrusion scenarios before a real incident tests it.

Every organization should revisit its cyber program at least once a year and whenever the business changes: a new acquisition, a new vendor, a new AI tool. Where in-house teams are stretched, an outside adviser can assess current and future risks, test defenses, and help respond when an incident happens. For PE firms managing risk across a portfolio, a structured approach to cybersecurity oversight is no longer a differentiator. It is table stakes.

HOW KAUFMAN ROSSIN CAN HELP

Our cybersecurity practice is built on a simple principle: you cannot protect what you do not understand. We start by identifying and quantifying your risk, then build and execute a program around it. Where your risk profile calls for specialized technology, we deploy proven solutions through our partner ecosystem.

01 / Start here

QUANTIFIED RISK ASSESSMENT

Start with a clear, dollar-denominated picture of your cyber risk. We map your environment against the frameworks that apply to your industry (NIST CSF 2.0, HIPAA, Regulation S-P, ISO, and others) and give your leadership team findings they can act on, not a generic checklist. For PE firms, we assess portfolio companies at acquisition and on a recurring basis so risk is visible across the fund.

02

PROGRAM DESIGN

Turn assessment findings into a prioritized roadmap. We design the policies, controls, and governance structures your organization needs, tailored to your size, industry, and risk appetite. This includes incident response planning, vendor oversight programs, and AI use policies.

03

IMPLEMENTATION

Execute the roadmap. From deploying Zero Trust architectures and MFA to running phishing and deepfake simulations, we handle the technical work so your team can stay focused on the business.

04

RETAINED ADVISORY

Stay ahead of what changes next. Our retained advisory relationships provide continuous monitoring guidance, regulatory change tracking, and a direct line to our team when an incident occurs.

05

SOC REPORTS AND COMPLIANCE

SOC 1 and SOC 2 examinations, HIPAA/HITECH readiness, and global data privacy compliance for organizations that need to demonstrate their security posture to customers and regulators.

PARTNER-POWERED SOLUTIONS

Continuous cyber risk management requires the right technology. We select, deploy and manage specialized tools through our partner ecosystem so that each solution is configured to your environment and integrated into your broader risk program. Our current partnerships include:

SYNACK

Continuous, AI-powered penetration testing by vetted offensive security researchers

NETRISE

Firmware and software supply chain risk analysis across IoT, OT and connected devices

REMEDIO

Automated IT asset discovery, vulnerability management and compliance mapping

The partner provides the technology. We bring the client context, the process discipline, and the integration with your broader risk program that helps you get full value from every investment.

WANT TO LEARN MORE?

Contact our cybersecurity team to talk about where your organization stands and what to prioritize next.



KORY PATRICK, CISSP
Cybersecurity Practice Leader
Principal, Risk Advisory Services
kpatrick@kaufmanrossin.com

SOURCES

- IBM, Cost of a Data Breach Report 2026 (July 2026) and 2025; summaries via IBM, eSecurity Planet, Baker Donelson, and SecureWorld
- Verizon, 2026 Data Breach Investigations Report (May 2026); summaries via TechRepublic and Abnormal AI
- IBM X-Force Threat Intelligence Index 2026
- Black Kite, “Mid-Market Is the Routine Target: Ransomware, Third-Party Risk, and the Widening AI Gap” (August 2026); analysis of 13,336 ransomware incidents, January 2023 through June 2026
- Coveware by Veeam, Q2 and Q3 2025 Ransomware Reports
- Kroll, “Cyber Risk at Scale: Safeguarding Portfolio Value in Private Equity” (February 2026); survey of 325 portfolio leaders
- ACA Group, “2026 PortCo Cyber Risk Report” (March 2026); assessments of 300+ portfolio companies across 18 industries and 12 countries
- Beazley, Risk & Resilience: Cyber Threat and Tech Advances 2026 (April 2026)
- SEC Regulation S-P amendments; alerts from Holland & Knight, Davis Wright Tremaine, and Parker Poe
- HHS proposed HIPAA Security Rule (January 2025); Fierce Healthcare and Paubox on the July 2027 timeline
- FFIEC statement on the Cybersecurity Assessment Tool sunset
- Public reporting on the April 2025 Marks & Spencer incident

This report is for general information only and is not legal or technical advice for any specific situation.



kaufmanrossin.com
kpatrick@kaufmanrossin.com

Independent by choice. Accountable to you.
