What Midyear Trends Are Telling Us About Cyber Risk In 2026

By David Chavez, Product Manager, Information Technology Solutions, Intact Insurance Specialty Solutions

More than halfway through 2026, it still feels like every time you turn a corner in cyber, there's something new to deal with. The environment is more connected than ever, technology is moving fast, and everything ties together in ways that aren't always easy to see.

AI, third-party dependencies, and infrastructure concentration are now part of the day-to-day, and they're changing how teams think about exposure and resilience.

Preparation has evolved too. Protecting businesses from today's risks requires leaders to maintain a clear view of where exposure sits, keep governance tight, and be confident your response will hold up when something happens.

Here's where trends in cyber risks stand, and what's likely to shape the rest of the year.

AI Driven Risk Is Expanding the Attack Surface

AI has moved quickly from experimentation into everyday use. Large language models, agentic systems, and AI-enabled workflows are now embedded across organizations, improving productivity while bringing new governance and data challenges.

Most challenges start with visibility. Many teams still don't have a clear view of which tools are being used, what data is going into them, or how outputs are feeding into decisions. That visibility is what allows teams to apply meaningful governance.

At the same time, the underlying threats haven't changed. Claims and incident data still point to phishing, impersonation, and fraudulent instructions as major drivers of breaches. What's changing is how effective they are and how quickly the tactics can be deployed. AI makes these tactics faster to produce, easier to scale, and more convincing.

Limited transparency into how some models generate outputs adds another layer of complexity, especially for teams trying to validate results or document decisions. Without proper oversight and guardrails, employee use of these models could result in exposure and liability.

As AI adoption picks up, most organizations are focusing on a few core areas to stay protected:

- **Mapping AI usage across the environment:** Identifying approved tools, shadow AI activity, and where sensitive data is being entered
- **Defining data guardrails:** Setting clear boundaries around what data can be used in AI tools
- **Extending third-party risk reviews to AI:** Evaluating how vendors use AI and what data those systems access
- **Training employees on AI-enabled fraud:** Helping teams recognize deepfake calls, synthetic emails, and more sophisticated phishing attempts

Organizations that understand how AI is actually being used are in a much better position to govern it effectively and avoid surprises.

Hidden Dependencies Are Expanding Exposure Across Ecosystems

AI is adding complexity internally. At the same time, external dependencies are introducing risk that sits outside direct control. Most environments rely on layers of vendors, cloud platforms, APIs, and service providers, and visibility often drops off beyond primary relationships.

That structure changes how incidents play out. A single outage, misconfiguration, or compromise can ripple outward and affect multiple organizations at once. This becomes more pronounced as workloads concentrate within a small number of providers, creating shared exposure that teams are still working to fully understand.

As a result, traditional vendor management doesn't fully reflect how risk behaves. More organizations are shifting toward a dependency-based view. That typically includes:

- **Understanding vendor access paths:** Documenting which third parties connect to critical systems and how access is controlled
- **Identifying downstream dependencies:** Understanding where fourth-party exposure exists (who are your vendors outsourcing to?)
- **Enforcing consistent access controls:** Applying MFA, least privilege, and segmentation to third-party access
- **Assessing concentration risk:** Evaluating reliance on specific providers, regions, or platforms
- **Testing failover scenarios:** Validating recovery processes under real disruption conditions

Resilience increasingly depends on being ready for systemic disruptions that originate outside your environment.

Claims Data Shows How Attacks Exploit Trust and Process Gaps

As cyber risks materialize, claims data gives a clearer view of how incidents actually unfold.

Ransomware and business email compromise (BEC) still drive most losses, though the way they play out continues to shift.

Data exposure is increasingly becoming the central risk in ransomware incidents. Even when systems are restored, stolen data gives attackers ongoing leverage. Organizations are negotiating over disclosure as much as recovery, and incidents are affecting a broader range of systems and business functions.

You see that shift in negotiations. Attackers are starting with higher demands and working down. Settlements can still be reduced, but it's getting harder to push them to lower levels.

BEC activity remains steady but more coordinated. In many cases, it's not just one email—requests are reinforced through calls, timing, or compromised accounts to create a stronger sense of legitimacy.

There are also early signs of AI showing up in claims, both in how attacks are carried out and how tools are being used internally without clear oversight.

Across incidents, the pattern is consistent: timing, trust, and process gaps create the opening, often at the human level.

Organizations that limit impact stay disciplined in a few areas:

- **Verifying payment changes independently:** Confirming instructions through known contacts or secondary channels before transferring funds
- **Recognizing coordinated fraud patterns:** Spotting when multiple touchpoints reinforce legitimacy
- **Preparing for data exposure:** Planning for extortion and disclosure, not just system recovery. This includes coordination with forensic, legal and communication teams and regularly deleting sensitive or unnecessary information so attackers have less valuable data to steal

- **Escalating anomalies in real time:** Ensuring unusual requests are flagged before potentially damaging action is taken

These controls aren't new, but they make a material difference in prevention and recovery.

AI and Vendor Risk Are Reshaping Cyber Insurance Underwriting

These trends are beginning to shift underwriting and the cyber insurance landscape as well.

The market remains broadly competitive, but underwriting scrutiny is tightening around AI uncertainty, third-party dependencies, and infrastructure concentration. In some cases, carriers are limiting or excluding exposures that are harder to define.

Conditions are still relatively soft, but there's more selectivity when governance is unclear or exposures are difficult to model.

For security leaders, the takeaway is straightforward: the strength of the control environment directly influences how risk is assessed, priced, and transferred.

Where to Focus for the Rest of 2026

The second half of the year will likely bring more change than clarity.

AI will keep evolving, dependencies will deepen, and attackers will keep adapting. Staying ready comes down to a few fundamentals: knowing where exposure sits, keeping core processes tight under pressure, and making sure response plans hold up in practice.

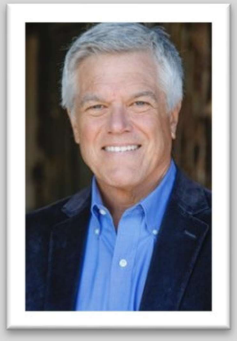
Those fundamentals are what hold when everything else is moving, and they're increasingly what separate organizations that absorb disruption from those that amplify it.

About Intact Insurance Specialty Solutions: Intact Insurance Specialty Solutions is the marketing brand for the insurance company subsidiaries of Intact Insurance Group USA LLC, a member of Intact Financial Corporation (TSX: IFC), the largest provider of property and casualty insurance in Canada, a leading provider of global specialty insurance, and, with RSA, a leader in the U.K. and Ireland. The insurance company subsidiaries of Intact Insurance Group USA LLC include Atlantic Specialty Insurance Company, a New York insurer, Homeland Insurance Company of New York, a New York insurer, Homeland Insurance Company of Delaware, a Delaware insurer, OBI America Insurance Company, a Pennsylvania insurer, and OBI National Insurance Company, a Pennsylvania insurer. Each of these insurers maintains its principal place of business at 605 Highway 169 N, Plymouth, MN 55441. For information about Intact Insurance Specialty Solutions products and services available in Canada, visit intactspecialty.ca, and for information about Intact Financial Corporation, visit intactfc.com.

This article is provided for general informational purposes only and does not constitute and is not intended to take the place of legal or risk management advice. Readers should consult their own legal counsel or other representatives for such advice. Any and all third-party websites or sources referred to herein are

for informational purposes only and are not affiliated with or endorsed by Intact Insurance Group USA LLC ("Intact"). Intact hereby disclaims any and all liability arising out of the information contained herein.

About the Author



David Chavez is Product Manager for Intact Insurance Specialty Solution's Technology business, with more than 30 years of experience in technology, cybersecurity, and insurance. He is a California attorney and certified cybersecurity professional specializing in cyber insurance and data breach risk management.

David can be reached at the company website: https://www.intactspecialty.com/