# **The Confluence of Fragility: From Digital Dependencies to Systemic Economic and National Security Crises**

## **Executive Summary: The Confluence of Physical and Digital Fragility**

The modern, interconnected economy is characterized by a paradox: systems designed for unprecedented efficiency have simultaneously created a profound and pervasive fragility. This report analyzes this new risk calculus by examining two emblematic incidents: the cyberattack on United Natural Foods, Inc. (UNFI) and the data breach at third-party vendor TeleMessage. These events, while seemingly disparate in their nature and impact, are not isolated occurrences but rather symptomatic examples of a single, systemic vulnerability. The central thesis is that digital infrastructure has become a critical point of failure, with a single IT disruption at a key distributor capable of causing nationwide physical shortages and a security flaw at a third-party vendor able to compromise national security.

The UNFI cyberattack demonstrated in stark terms how a digital failure can have devastating, tangible consequences. By crippling the IT systems of a major wholesale food distributor, the attack led directly to operational shutdowns, delivery delays, and empty grocery store shelves across North America. This incident underscored the critical, yet often unappreciated, role of a single entity in a complex supply chain and exposed the systemic risks embedded within the food and agriculture sector. Simultaneously, the TeleMessage breach revealed a different, but equally significant, dimension of digital fragility. A seemingly minor technical misconfiguration in a vendor’s system exposed sensitive communications and metadata from over 60 U.S. government agencies. This compromise did not involve a simple data dump; rather, it constituted a profound counterintelligence threat, providing a detailed blueprint of communication patterns for potential adversaries.

The analysis in this report synthesizes these findings to demonstrate a unified threat. It argues that the pursuit of hyper-efficiency, through practices like just-in-time (JIT) logistics and the concentration of both physical and digital power in a few key entities, has amplified fragility. The solution requires a fundamental strategic shift. This report provides a multi-layered set of recommendations, including enhancing third-party risk management (TPRM), building operational resilience through diversification, and implementing robust cybersecurity governance frameworks. The report's findings compel a move from a reactive, siloed approach to a proactive, holistic strategy that prioritizes resilience and robust oversight across the entire interconnected ecosystem.

## **Section 1: The Modern Supply Chain's Achilles' Heel**

### **Defining Supply Chain Fragility**

Supply chain fragility, in its most fundamental designation, is the susceptibility of a supply chain to disruptions.1 This concept is not merely a theoretical weakness but a very real condition that leads to tangible consequences such as empty shelves, production halts, and significant price fluctuations.1 A supply chain is an interconnected network of resources, processes, and entities that move goods from their origin to the final consumer.1 Fragility, when applied to this system, denotes a lack of robustness and an inherent tendency to break under pressure from unforeseen challenges, even if the system operates with peak efficiency under normal conditions.1

The vulnerability of this complex system can be broken down into its key operational components. Fragility at the **sourcing** stage can stem from a reliance on single suppliers or geographically concentrated sources, creating significant dependency and a critical point of failure.1 In

**manufacturing**, the vulnerability often arises from the widespread adoption of 'just-in-time' (JIT) inventory systems, which minimize warehousing costs but leave little to no buffer to absorb shocks.1 The pursuit of lean management processes, such as JIT, requires an entire business workflow to convert to a lean framework, and any breakdown in a single part of that intricate arrangement can jeopardize the entire infrastructure.3 Similarly, the

**logistics and distribution** stages are susceptible to exposure from disruptions to shipping routes, port congestion, or warehousing capacity limitations.1 This final stage, getting products to the end consumer, can also be fragile due to "last-mile" delivery issues or retail network vulnerabilities.1

From an academic perspective, the definition of supply chain fragility transcends a mere operational concern and becomes a subject of strategic, economic, and even geopolitical analysis.1 At this level, fragility is viewed not simply as a matter of individual weak links, but as a "systemic instability and cascading failure potential" inherent in complex, interconnected systems.1 The contemporary understanding of supply chains recognizes them as dynamic, complex adaptive networks that exhibit emergent properties.1 Within this framework, small perturbations can trigger disproportionately large and cascading failures, leading to significant deviations from expected performance or even complete system collapse.2 This nuanced interpretation incorporates the broader connotation of systemic risk, implying that vulnerabilities are not isolated but are deeply embedded within the structural and operational paradigms of modern supply networks.1

### **The Digital Dependency Paradox**

The unprecedented efficiency of modern supply chains is enabled by seamless connectivity, which facilitates the flow of materials, information, and financial resources.4 However, this deep digital integration has created a new, profound source of vulnerability. Digital systems, which are meant to enable efficiency, have become a "conduit for cascading failures when stressed".2 The interconnectedness that drives economic benefits in stable times is the same force that can rapidly propagate a disruption across an entire network.2 This interdependence is particularly acute in critical sectors, where a single IT failure can cause a physical supply chain to grind to a halt.5

A critical dimension of this dependency is the concentration of digital power. While global discussions often focus on traditional trade imbalances, there has been insufficient scrutiny of the "digital hegemony" exerted by a limited number of technology companies.6 A handful of US companies, including Google, Amazon, Meta, Apple, and Microsoft, control the world's essential digital infrastructure, from search to cloud services to mobile platforms.6 This concentration creates systemic points of failure, as a disruption at a dominant cloud provider, for example, can cascade across thousands of organizations and ecosystems that depend on its services.7

This concentration also makes digital infrastructure a new lever of economic and geopolitical coercion. Unlike physical infrastructure, digital platforms can be modified or weaponized at a much faster pace, creating new dynamics in international relations.6 The report cites examples such as Elon Musk's Starlink decisions affecting Ukraine's military communications and app stores' power to eliminate services from entire populations.6 This dynamic raises fundamental questions about economic autonomy and sovereignty when essential functions depend on foreign-controlled platforms.6 Nations face a choice: accept this "digital vassalage" or invest in building their own independent digital infrastructure.6 The TeleMessage incident, as will be discussed, demonstrates how this digital dependency can directly translate into national security risks.

The blurring line between information technology (IT) and operational technology (OT) is a key element of this paradox. Modern manufacturing and logistics systems are increasingly computerized, with core operational functions tied directly to network-based IT infrastructure.8 This means that a cyberattack targeting an IT system, such as a warehouse management platform or an order-management system, can have an immediate and direct impact on the physical operational environment, such as a production line or a distribution center.8 The fragility of the digital layer is therefore an inseparable part of the fragility of the physical supply chain. Risk management strategies that fail to account for this integrated reality are fundamentally incomplete.

## **Section 2: Case Study in Physical Disruption - The UNFI Cyberattack**

### **The Incident and Immediate Fallout**

On June 5, 2025, United Natural Foods, Inc. (UNFI), the largest publicly traded wholesale food distributor in North America, detected unauthorized activity on its IT systems.8 In response, the company immediately activated its incident response plan and took critical systems offline to contain the breach.8 The systems impacted included those managing warehouse operations, transportation logistics, and order management.8

The operational disruption was immediate and severe. Deliveries were delayed, employee shifts were canceled, and a widespread cyber outage affected over 30,000 retail locations.8 To maintain limited operations, UNFI was forced to implement manual workarounds, including using paper and pen to track deliveries and fulfill orders where possible.8 Although UNFI began to restore its primary electronic ordering systems within ten days and its core systems by late June, disruptions persisted for several weeks.8

The financial repercussions were substantial. UNFI expected the cyberattack to cost it between $350 million and $400 million in lost sales.15 The company also incurred an estimated $20 million in expenses for implementing manual processes and preventing spoilage, along with another $5 million for cybersecurity experts, legal assistance, and other remediation costs.15 The incident was expected to result in a net income loss of up to $60 million for the quarter.15 While UNFI's cyber insurance policy was expected to cover the recovery and remediation expenses, the company noted that reimbursement would likely not arrive until the following fiscal year.13

### **The Ripple Effect on the Economy**

The UNFI cyberattack provides a powerful example of how a concentrated point of failure in a non-IT sector can have a devastating, nationwide impact. UNFI's position as the primary supplier to Whole Foods and a key distributor to over 30,000 retailers underscores its role as a critical node in the North American food supply chain.8 The attack on this single entity did not just affect one company; it caused a ripple effect that led to "empty store shelves across thousands of grocery locations".8 This outcome highlights the systemic risk that arises from market concentration, where the vulnerability of one part of the system threatens the stability of the whole.

The impact on independent grocers varied significantly based on their reliance on UNFI and their ability to find alternative suppliers.14 For Darlings Grocery, which sourced about two-thirds of its products from UNFI, the attack forced a scramble to find alternatives like Mason Brothers, which could not provide the same range of organic products, leading to empty shelves.14 This situation illustrated a critical weakness: the reliance on a single primary distributor for better pricing and a full selection of specialized products.14

Conversely, other grocers demonstrated greater resilience. Orcas Food Co-op, which sourced products from dozens of local suppliers, was less impacted and was able to turn to third-party suppliers with relative ease.14 Similarly, Charley Family Shop 'n Save quickly contacted organizations like the National Grocers Association, which helped them connect with an alternative wholesaler.14 This quick action, combined with pre-existing relationships with local suppliers, allowed the store to remain almost fully stocked.14

The UNFI incident also highlights a deeper issue regarding the pursuit of market efficiency. For decades, supply chains have been optimized to be lean and cost-effective, with practices like JIT logistics.3 However, this hyper-efficiency comes at the cost of redundancy, leaving no buffer when a critical supplier experiences a disruption.2 The grocers who were most affected by the UNFI attack were those that lacked pre-existing alternative suppliers or a sufficient inventory buffer. The attack on a logistics company's IT systems, which caused physical food shortages, demonstrated that for critical infrastructure sectors like food and agriculture, the distinction between IT and operational fragility is functionally obsolete. This necessitates a strategic re-evaluation of the balance between efficiency and resilience, with a greater emphasis on building redundancy and alternative sourcing options into the operational model.17

## **Section 3: Case Study in Strategic Compromise - The TeleMessage Breach**

### **The Technical Vulnerability and Exploit**

The TeleMessage breach, which occurred in May 2025, was a significant event that exposed a deep-seated vulnerability in third-party vendor security. The technical root cause was a fundamental security misconfiguration rather than a complex, state-of-the-art attack.19 A hacker exploited a publicly accessible Spring Boot Actuator

/Heap Dump endpoint on one of TeleMessage's archive servers.19 This endpoint, designed for debugging purposes, should never have been exposed to the public internet.19

By downloading a memory dump of the running application, the hacker was able to extract highly sensitive data in plaintext. This included usernames, passwords, encryption keys, and active session tokens for TeleMessage's backend and archive systems.19 With these credentials, the hacker was able to gain access to administrative dashboards, from which they downloaded archived message logs from various clients and exported contact lists and metadata.19 This exploit, which reportedly took less than 30 minutes, underscores the precariousness of modified messaging systems that are not configured with robust security controls.19

### **The Data at Risk and Its Context**

The scope of the breach was extensive, impacting both financial institutions and government agencies. Financial firms such as Coinbase, Scotiabank, and Galaxy Digital were affected, with the exposure of staff communications and credentials that could be used for targeted phishing attacks.19 However, the most profound implications were in the government sector. The breach compromised metadata and archived communications from over 60 U.S. government agencies, including FEMA, U.S. Customs and Border Protection (CBP), the U.S. Secret Service, White House staff, and the U.S. Diplomatic Corps.19

A key factor in this breach was TeleMessage's business model, which created a tension between regulatory compliance and security.20 The company was known for creating modified versions of encrypted messaging applications to meet government archiving mandates for eDiscovery and oversight.20 This compliance-driven modification, which involved capturing messages post-decryption for archival purposes, "undermined the very security these tools were built to ensure".20 This contradiction reveals a critical failing: organizations often treat compliance as the end-goal of security, but this incident demonstrates that meeting regulatory checkboxes does not always equate to building truly robust and resilient systems.

### **National Security Implications**

The TeleMessage breach represents a major counterintelligence risk, with the true danger lying not just in the content of the messages but in the exposed metadata.21 While the intercepted messages were often fragmentary and did not expose classified content, the metadata can reveal invaluable insights into the operational footprints, timelines, connections, and affiliations of key agencies and officials.21 For adversaries, this information provides a detailed blueprint for tracking communication channels and predicting government movements and operations, turning seemingly fragmented data into strategic intelligence.22

This incident is a textbook example of a failure in operational security. It highlights how the use of a lesser-known, third-party messaging platform was driven by convenience in procurement and bureaucratic inertia, rather than a rigorous, risk-based security assessment.21 The Cybersecurity and Infrastructure Security Agency (CISA) swiftly urged agencies to stop using the application, emphasizing the significant counterintelligence risks posed by the breach.21 The event demonstrates that the new front line of geopolitical conflict is often the third-party vendor. Adversaries do not need to breach the firewalls of a government agency directly; they can target a smaller, less-secure vendor that has trusted access to sensitive data.23 This approach represents a new form of asymmetric warfare, where a single vulnerability in a seemingly benign vendor can have profound national security consequences.

## **Section 4: Synthesizing the Threat - From Empty Shelves to Counterintelligence Risks**

### **The Common Thread: A Failure in Third-Party Risk Management**

The UNFI and TeleMessage incidents are powerful, real-world examples of a fundamental breakdown in third-party risk management (TPRM). Although one attack led to physical disruptions and the other to a data breach, both were manifestations of the same systemic vulnerability: a critical dependency on a third-party partner whose security posture was inadequate.23 The grocers who relied on UNFI were exposed to the risk of their key supplier's operational systems being compromised, which directly impacted their business continuity. Simultaneously, the government agencies that used TeleMessage were exposed to the risk of a vendor's technical flaw compromising their sensitive data and communications.

This analysis concludes that both incidents are textbook examples of a "supply chain attack," where an organization's operations or data are compromised via a vulnerability in a vendor, contractor, or service provider.23 The specific nature of the compromise—whether a financial loss from an operational shutdown or a national security risk from metadata exposure—is secondary. The root cause is the same: a failure to adequately vet, monitor, and manage the security risks posed by third-party relationships.

### **The Drivers of Systemic Vulnerability**

A critical driver of this systemic vulnerability is what has been termed "cyber inequity".7 The resilience of an entire ecosystem is often determined by its weakest link, which is frequently a smaller organization with insufficient resources to maintain adequate security standards.7 While large organizations may improve their own cyber resilience, a smaller partner with limited resources, like the third-party messaging vendor TeleMessage, can become the entry point for a wider attack.7 To counter this, larger, more resource-rich organizations must recognize that their security posture is a shared responsibility and support their smaller partners in meeting security standards.7

The UNFI incident highlighted the perilous nexus between JIT logistics and digital dependency. The JIT model, which minimizes inventory and production buffers, was originally designed for a less digitally-connected world.3 When this highly efficient but fragile physical supply chain becomes critically dependent on a similarly fragile digital layer, as seen with UNFI's IT systems, the risk is multiplied exponentially.3 A disruption that might have been mitigated by a small inventory buffer in a JIT-free world becomes a nationwide crisis when the digital system responsible for orders and logistics is taken offline.8

The report also identifies a convergence of threats, where the line between financially-motivated cybercrime and geopolitically-motivated attacks is blurring. The UNFI attack, while possibly tied to a financially motivated group like Scattered Spider 15, echoes the operational disruptions seen in attacks on other critical infrastructure, such as the Colonial Pipeline and Change Healthcare incidents.5 In the Colonial Pipeline attack, an IT-targeted ransomware attack forced an 11-day shutdown of an OT system, causing fuel shortages and panic buying.5 The Change Healthcare attack similarly disrupted billing and prescription processing for weeks, highlighting how deeply the healthcare system relies on digital infrastructure.5 These incidents demonstrate that the tools and tactics of cyberattacks are increasingly being used to achieve a wide variety of strategic ends, blurring the line between financial crime and threats to national security and public welfare.

| Incident Type | Victim | Nature of Compromise | Immediate Impact | Downstream Impact | Root Cause | Key Insight |
| --- | --- | --- | --- | --- | --- | --- |
| Cyberattack | UNFI (Logistics) | IT systems failure (order management, warehouse robotics) 8 | Operational shutdown, delivery delays 8 | Physical shortages for thousands of grocers and consumers 8 | Undisclosed (likely ransomware) 8 | Digital fragility causes physical disruption 8 |
| Data Breach | TeleMessage (Vendor) | Security flaw in public-facing endpoint and archive system 19 | Data exposure, including credentials and metadata 19 | National security risk for 60+ government agencies 19 | Misconfigured public debugging endpoint 19 | Third-party vendor flaw creates national security risk 21 |

*Table 1: Comparative Analysis of UNFI and TeleMessage Incidents*

## **Section 5: Building Resilience in an Interconnected World**

### **Enhancing Third-Party Risk Management (TPRM)**

Given the systemic risks posed by third-party dependencies, TPRM is no longer a compliance function but a strategic imperative.24 The goal is not to avoid vendor relationships but to engage exclusively with partners who demonstrate a robust security posture.24 To achieve this, organizations must implement a comprehensive and proactive TPRM program that moves beyond one-time assessments.27

A fundamental first step is **risk-based segmentation**, or tiering, of all vendors based on the criticality of their services and their access to sensitive data.24 This allows organizations to efficiently allocate limited time and resources to the relationships that pose the highest risk.24 For high-risk vendors, a more rigorous due diligence process is essential.27 This should include standardized questionnaires, document reviews (e.g., attestation to ISO 27001 or SOC 2 certifications), and the use of third-party intelligence feeds to evaluate their cybersecurity posture, financial stability, and compliance history.24

Crucially, organizations must move from a point-in-time assessment model to **continuous monitoring** of their vendors' security postures.24 Automated platforms can provide dashboard views of vendor health and issue alerts the moment risk is discovered, helping to detect evolving threats.24 The scope of this oversight must also be extended to

**fourth parties**, or sub-contractors, as risk can cascade quickly across the entire supply chain ecosystem.24 To manage this complexity, investing in IT tools that centralize vendor data, automate workflows, and provide real-time analytics is critical for scaling a TPRM program with limited resources.26

### **Strategies for Operational Resilience**

The UNFI incident provided a clear justification for strategic investments in operational resilience. The first step is to adopt **supplier diversification and multi-sourcing** to mitigate the risk of relying on a single vendor.2 This can be accomplished by negotiating with multiple suppliers, spreading the business among them so that no single supplier has more than 30-40% of the volume, and strategically pursuing nearshoring or onshoring to reduce geopolitical and logistical risks.17

Organizations must also reassess their **inventory management strategies**.29 The JIT model, while efficient, proved to be highly vulnerable to disruption.3 A more resilient approach involves a shift to a "just-in-case" (JIC) model or a hybrid strategy that prioritizes safety stock.29 By maintaining buffer quantities of critical items based on historical data, companies can avoid stockouts and maintain business continuity during disruptions.28

Finally, **proactive risk assessment and contingency planning** are non-negotiable.28 Organizations should identify weak spots, such as single points of failure, and develop specific contingency protocols for various disruption scenarios.17 This requires leveraging technology for end-to-end visibility and real-time tracking across the supply chain, which provides the necessary data and analytical power to respond quickly and coordinate with partners in an emergency.28

*Table 2: Key Strategies for Resilience and Risk Management*

| Strategy Category | Specific Action | Goal | Rationale |
| --- | --- | --- | --- |
| **Third-Party Risk Management** | Risk-based Segmentation | Efficiently allocate resources | Focuses due diligence on critical, high-risk vendors who have access to sensitive systems or data.24 |
|  | Continuous Monitoring | Detect evolving threats | Moves beyond one-time assessments to provide a real-time view of a vendor's security posture throughout the contract.24 |
|  | Extend to Fourth Parties | Mitigate cascading risks | Addresses the fact that a company's risk exposure can extend beyond its direct vendors to their sub-contractors and partners.24 |
| **Operational Resilience** | Supplier Diversification | Mitigate single-supplier risks | Reduces dependency on a single source, ensuring supply continuity during disruptions caused by cyberattacks, natural disasters, or geopolitical events.18 |
|  | Rebalance Inventory | Create operational buffers | Shifts from a hyper-efficient 'just-in-time' model to a hybrid approach that maintains 'safety stock' for critical items to absorb shocks.3 |
|  | Proactive Contingency Planning | Enable a rapid response | Involves conducting scenario analyses and developing clear protocols for disruptions to minimize operational downtime and financial losses.28 |
| **Cybersecurity Governance** | Adopt Formal Frameworks | Standardize security practices | Provides a structured, holistic approach to managing cyber risk and demonstrates a mature security posture to stakeholders.30 |
|  | Implement Zero-Trust | Limit lateral movement | Assumes no user or system is trusted by default, drastically reducing the potential blast radius of an attack, as seen in the TeleMessage breach.19 |

### **Cybersecurity Governance and Frameworks**

To secure the entire ecosystem, organizations must embed cybersecurity into their core governance and operational frameworks. The adoption of formal, widely-recognized standards like the **NIST Cybersecurity Framework 2.0** and **ISO 27001** is a critical step.30 NIST 2.0, for example, extends its reach beyond critical infrastructure and emphasizes cybersecurity governance as a key component of enterprise risk management alongside financial and reputational risks.30 An ISO 27001 certification, while a point-in-time exercise, can validate a mature cybersecurity program and demonstrate a commitment to risk management to customers, partners, and shareholders.30

The TeleMessage incident provides a compelling case for implementing a **Zero-Trust architecture**.19 A Zero-Trust model assumes that no system or user, whether inside or outside the network, is automatically trusted.22 This principle requires continuous verification of every access attempt, limiting the ability of a compromised credential to move laterally through the network and drastically reducing the potential blast radius of a breach.22

Finally, it is essential to recognize that cybersecurity is not solely the domain of technical experts. A robust defense requires a holistic approach that includes non-technical roles like risk management, compliance, and security awareness.31 Professionals in these roles are vital for identifying vulnerabilities, ensuring that security strategies align with business goals, and training employees to recognize and mitigate threats.31 As the TeleMessage breach demonstrated, the human element—whether through a technical misconfiguration or a lapse in protocol—remains a critical point of vulnerability that must be addressed with rigorous policies and a culture of security awareness.21

## **Conclusion: The Imperative for a Proactive Posture**

The analysis of the UNFI and TeleMessage incidents demonstrates that the fragility of the modern interconnected economy is not a theoretical concern but a present and profound reality. The report establishes that the distinction between physical and digital vulnerabilities is functionally obsolete, as a single IT failure can now trigger a cascading chain of physical, economic, and even national security crises. This new threat landscape is driven by the pursuit of hyper-efficiency, which has led to concentrated points of failure, both in physical logistics and digital infrastructure, and by a pervasive "cyber inequity" across the supply chain.

The reactive, siloed approach to risk management is no longer sufficient. Organizations and policymakers must adopt a proactive, holistic, and ecosystem-wide strategic posture that balances the benefits of efficiency with a profound and continuous commitment to resilience. The path forward is clear: a multi-layered strategy that includes a robust third-party risk management program, proactive operational resilience measures, and the adoption of modern cybersecurity governance frameworks. By implementing risk-based segmentation and continuous monitoring, diversifying suppliers and rebalancing inventory strategies, and embracing a Zero-Trust architecture, businesses and governments can build the resilient infrastructure necessary to endure and thrive in an increasingly uncertain and interconnected world. The UNFI and TeleMessage incidents serve as a powerful and urgent call to action, demanding a fundamental shift in mindset to one where resilience is not a cost center but a core strategic imperative.

#### Works cited

1. Supply Chain Fragility → Term - ESG → Sustainability Directory, accessed August 14, 2025, <https://esg.sustainability-directory.com/term/supply-chain-fragility/>
2. Supply Chain Fragility → Term - Fashion → Sustainability Directory, accessed August 14, 2025, <https://fashion.sustainability-directory.com/term/supply-chain-fragility/>
3. Just-in-Time (JIT) Inventory: A Definition and Comprehensive Guide ..., accessed August 14, 2025, <https://www.netsuite.com/portal/resource/articles/inventory-management/just-in-time-inventory.shtml>
4. The Connected Supply Chain - IADB Publications, accessed August 14, 2025, <https://publications.iadb.org/publications/english/document/The-Connected-Supply-Chain-Enhancing-Risk-Management-in-a-Changing-World.pdf>
5. Top 5 Cyberattacks on Critical Infrastructure | Microminder Cyber ..., accessed August 14, 2025, <https://www.micromindercs.com/blog/cyber-attacks-on-critical-infrastructure>
6. Digital dependency a hidden trade imbalance - Luxury Barbados Property for Sale, accessed August 14, 2025, <https://orianabarbados.com/digital-dependency-a-hidden-trade-imbalance/>
7. Cybersecurity: 5 risks from supply chain interdependencies | World ..., accessed August 14, 2025, <https://www.weforum.org/stories/2025/01/5-risk-factors-supply-chain-interdependencies-cybersecurity/>
8. The UNFI Cyberattack: What It Could Mean for You - TenHats, accessed August 14, 2025, <https://tenhats.com/the-unfi-cyberattack-updates-and-what-it-could-mean-for-you/>
9. Impact of modern ransomware on manufacturing networks - LevelBlue, accessed August 14, 2025, <https://levelblue.com/blogs/security-essentials/impact-of-modern-ransomware-on-manufacturing-networks>
10. Ransomware in Manufacturing | Supply Chain Ransomware - BullWall, accessed August 14, 2025, <https://bullwall.com/ransomware-in-manufacturing/>
11. UNFI Cyberattack Halts Deliveries to Whole Foods and 30,000+ Grocery Stores, accessed August 14, 2025, <https://www.vulnu.com/p/unfi-cyberattack-halts-deliveries-to-whole-foods-and-30-000-grocery-stores-021b>
12. UNFI Systems Update - United Natural Foods, Inc., accessed August 14, 2025, <https://ir.unfi.com/news/press-release-details/2025/statement/default.aspx>
13. United Natural Foods says week-long cyber incident will impact quarterly income, accessed August 14, 2025, <https://therecord.media/united-natural-foods-cyber-incident-q4-impact>
14. How the cyberattack against UNFI affected 4 independent grocers ..., accessed August 14, 2025, <https://www.grocerydive.com/news/unfi-cyberattack-response-supply-chain-grocery-wholesale/750831/>
15. United Natural Foods loses up to $400M in sales after cyberattack - CyberScoop, accessed August 14, 2025, <https://cyberscoop.com/united-natural-foods-cyberattack-400-million/>
16. UNFI expects cyberattack to cost it at least $350 million in sales ..., accessed August 14, 2025, <https://www.cybersecuritydive.com/news/unfi-cyberattack-losses-insurance-grocery-distribution/753224/>
17. Supplier diversification strategies to mitigate market risks - EOXS, accessed August 14, 2025, <https://eoxs.com/new_blog/supplier-diversification-strategies-to-mitigate-market-risks/>
18. Procurement 101: Supplier Diversification – Practical guide to driving it - CADDi, accessed August 14, 2025, <https://us.caddi.com/resources/insights/supplier-diversification>
19. How was TeleMessage hacked? Does this mean that all messaging ..., accessed August 14, 2025, <https://www.celltrust.com/telemessage-and-your-secure-compliant-mobile-comms-checklist/>
20. The TeleMessage Breach: A Cautionary Tale of Compliance Versus Security, accessed August 14, 2025, <https://complexdiscovery.com/the-telemessage-breach-a-cautionary-tale-of-compliance-versus-security/>
21. Inside the TeleMessage Breach: Lessons in Government Communication Security, accessed August 14, 2025, <https://cybercover.sg/2025/inside-the-telemessage-breach-lessons-in-government-communication-security-and-metadata-risks/>
22. TeleMessage Breach Exposes U.S. Government Metadata, accessed August 14, 2025, <https://zendata.security/2025/05/25/hacker-breach-of-trump-aides-messaging-app-exposed-data-from-over-60-us-government-officials/>
23. Third-Party Data Breach: Examples and Prevention Strategies - Legit Security, accessed August 14, 2025, <https://www.legitsecurity.com/aspm-knowledge-base/third-party-data-breach>
24. Third-Party Data Breach: Definition & 5 Examples | Bitsight, accessed August 14, 2025, <https://www.bitsight.com/blog/third-party-data-breach>
25. Logistics Risk Management for Just-In-Time Auto Supply Chains - One Union Solutions, accessed August 14, 2025, <https://oneunionsolutions.com/blog/logistics-risk-management-for-just-in-time-auto-supply-chains/>
26. Third-party risk management in 2025: How to build a scalable program, accessed August 14, 2025, <https://www.diligent.com/resources/guides/third-party-risk-management>
27. Improving third-party risk management - McKinsey, accessed August 14, 2025, <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Improving%20third%20party%20risk%20management/Improving-third-party-risk-management.ashx>
28. How to build supply chain resilience | Maersk, accessed August 14, 2025, <https://www.maersk.com/logistics-explained/supply-chain-management/2024/02/21/building-a-resilient-supply-chain>
29. What Is Supply Chain Resilience? - IBM, accessed August 14, 2025, <https://www.ibm.com/think/topics/supply-chain-resiliency>
30. 7 Cybersecurity Frameworks to Reduce Cyber Risk in 2025 - BitSight Technologies, accessed August 14, 2025, <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>
31. Explore Non-Coding Cybersecurity Jobs & Career Paths| ECCU - EC-Council University, accessed August 14, 2025, <https://www.eccu.edu/blog/cybersecurity-jobs-that-dont-require-coding-exploring-non-technical-roles/>
32. 10 Nontechnical Cybersecurity Jobs - Coursera, accessed August 14, 2025, <https://www.coursera.org/articles/non-technical-cyber-security-jobs>