

Ransomware & Extortion

Preparing for Multifront Attacks

October 2026

forvis mazars

Today’s Presenters



Paul Truitt
Principal, IT Risk & Compliance
215.913.9968
paul.truitt@us.forvismazars.com



Justin Lance
Senior Manager, IT Risk & Compliance
704.367.7047
justin.lance@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Agenda

1. Setting the Scene
2. The Modern Extortion Playbook
3. Controls That Help Reduce Loss
4. Who You Must Tell & When
5. Executive Tabletop Walkthrough
6. Takeaways & Discussion



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Tabletop Scenario

The Voice-Cloned CEO Call

They Get In

Someone uses a stolen password, a phishing email, or an unpatched system to get inside. This often happens weeks before anyone notices.

They Take Copies

Before doing anything visible, they copy customer records, contracts, and email so they have something to threaten you with.

They Lock or Wipe

They encrypt or erase systems so the business stops working. Some attacks now skip the ransom and go straight to destruction.

They Apply Pressure

A demand arrives with a deadline. If you refuse, they call your customers, post samples online, or report you to regulators.

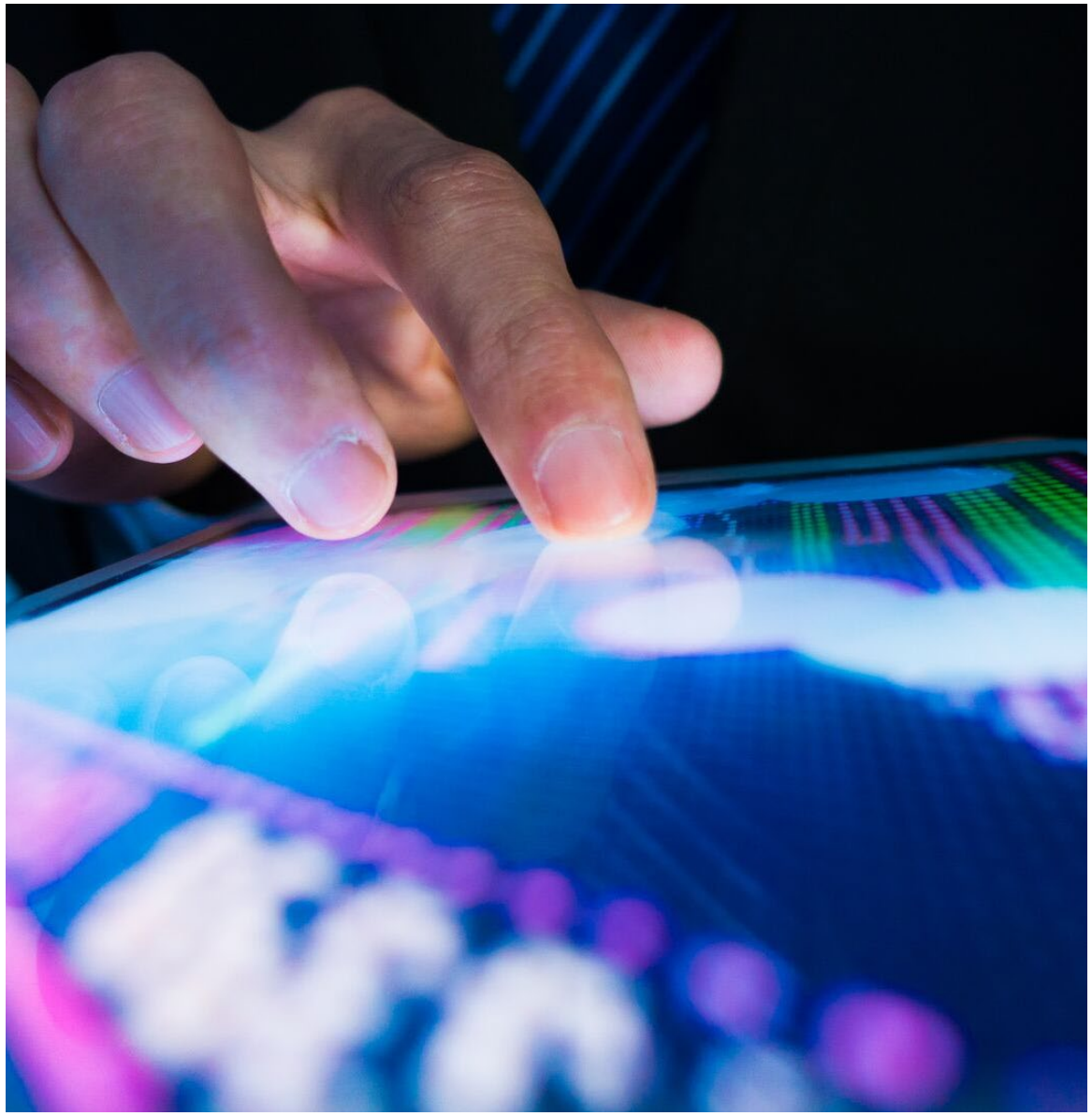
© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Setting the Scene
Why This Topic Matters Now

Ransomware and data theft now blend with supplier compromises and multi-party extortion, turning a single incident into a cascading business problem across operations, vendors, customers, and contracts.

Restoring systems and devices is only half the work. Stolen data and downstream fallout likely present bigger challenges.



Cost of a Breach

$11.5M

average U.S. breach cost, more than double the global figure.

According to IBM's 2026 Cost of a Data Breach report, ransomware appeared in roughly four in 10 breaches and the cost is growing.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Setting the Scene
Ransomware & Extortion Signals

39%

Hit by ransomware

Share of breached organizations hit by ransomware, a fourth straight year of increase.

41%

Reputation threats

Ransomware attacks that added threats to brand reputation to pressure victims into paying.

5.28x

Blast radius

Downstream companies publicly compromised, on average, for every single vendor breach.

25%

More victims YoY

Increase in publicly disclosed ransomware victims, a fourth consecutive record year.

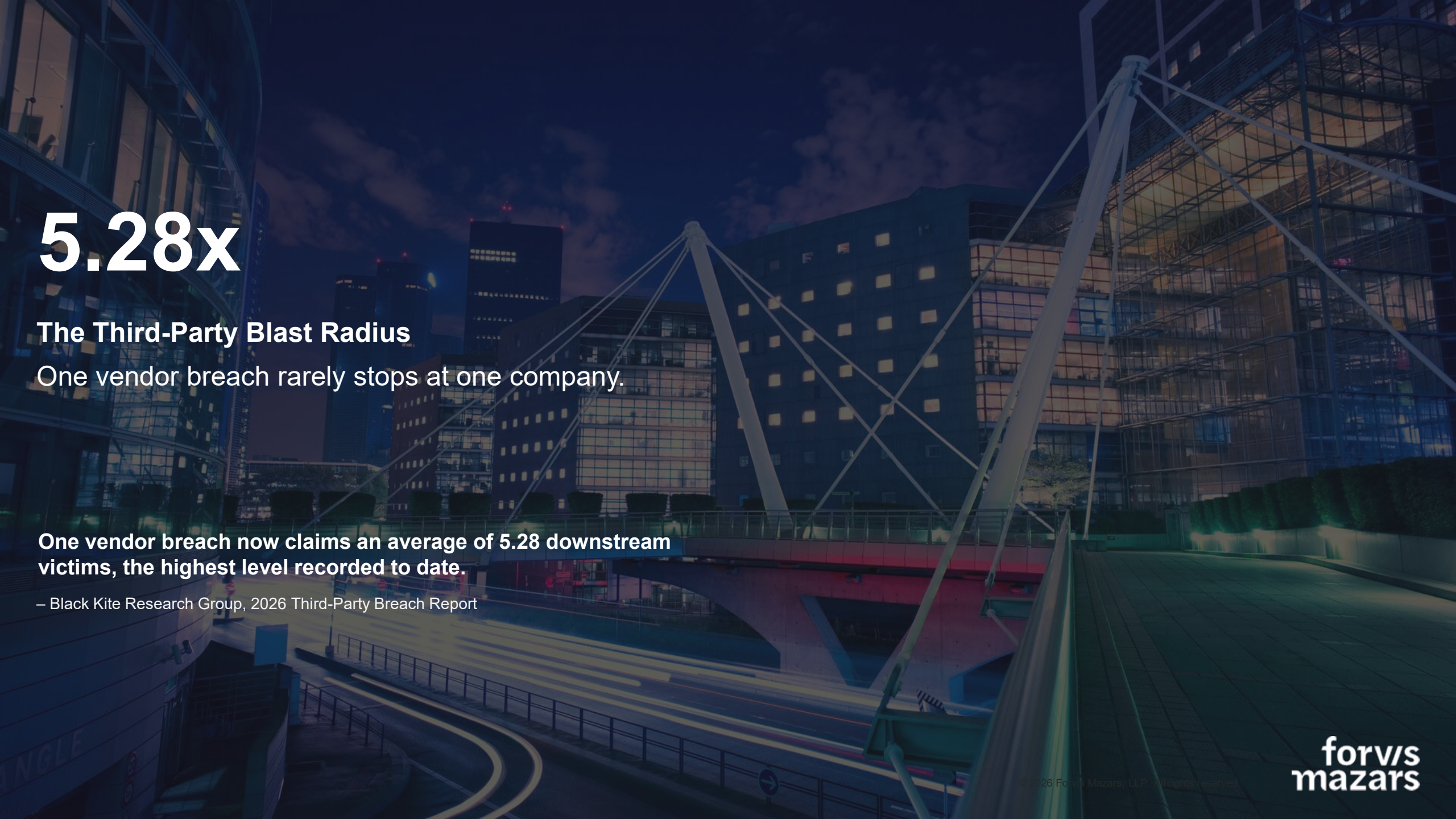
Extortion now extends beyond a single organization.

Attackers increasingly pair or replace encryption with data theft, then pressure suppliers, customers, and regulators. Supplier compromise amplifies the financial, legal, and operational exposure of one event.

Sources: IBM Cost of a Data Breach 2026; Black Kite 2026 Ransomware & Third-Party Breach Reports.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars



5.28x

The Third-Party Blast Radius

One vendor breach rarely stops at one company.

One vendor breach now claims an average of 5.28 downstream victims, the highest level recorded to date.

– Black Kite Research Group, 2026 Third-Party Breach Report

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Recent Public Incidents

Four events, one pattern: the damage lands far from the point of entry.

Stryker, March 2026

Attackers used an admin account to trigger the remote wipe built into the device management tool. No ransom, no malware; devices worldwide went dark for about a month.

CDK Global, June 2024

One software vendor for roughly 15,000 auto dealerships went down for two weeks. Dealers lost an estimated $1 billion and never had a breach of their own.

Marquis Software, August 2025

A year-old unpatched firewall at a marketing vendor led to ransomware. More than 74 banks and credit unions had to notify hundreds of thousands of customers.

Kettering Health, May 2025

Attackers sat inside a 14-hospital system for 41 days before locking its records system for two weeks. Lawsuits followed over delayed care.

Sources: Stryker Form 8-K (Mar 2026); TechTarget on CDK Global (2024); Maine AG notice and BleepingComputer on Marquis (2025); HIPAA Journal and The Record on Kettering Health (2025).

© 2026 Forvis Mazars, LLP. All rights reserved.

The Extortion Playbook
From Data Theft & Encryption to Multifront Pressure & Disruption

Data-Driven Extortion

Attackers copy data before encrypting, so restoring systems ends the outage but not the extortion.

Multi-Party Leverage

Attackers email your customers, post samples on leak sites, and report you to regulators to apply more pressure.

Operational Resilience

Cyber risk is a continuity issue, so response spans legal, communications, insurance, and business recovery.

Disruption-Focused Attacks

Some recent events demand no ransom at all, abusing legitimate admin tools to wipe devices and halt operations at scale.

© 2026 Forvis Mazars, LLP. All rights reserved.

Third-Party Blast Radius
How One Incident Can Cascade

Impact widens at each step. The entry point is rarely where the damage ends.

Suppliers A vendor breach becomes your incident when it touches your data or operations.

Customers Exposed data triggers notification duties, churn, and reputational harm.

Regulators Scrutiny follows the data, not the point of compromise.

© 2026 Forvis Mazars, LLP. All rights reserved.

Controls That Help Reduce Loss
Levers That Limit Extortion Impact

Identity Hardening

Phishing-resistant MFA, least privilege, and rapid access revocation reduce the credential abuse that starts most incidents.

Immutable Backups

Tamper-proof, tested backups preserve recovery options so the organization can decline to negotiate under duress.

Segmentation

Segmented, least-privilege connectivity limits lateral movement, especially from third-party access into core systems.

Supplier Risk & Contract Controls

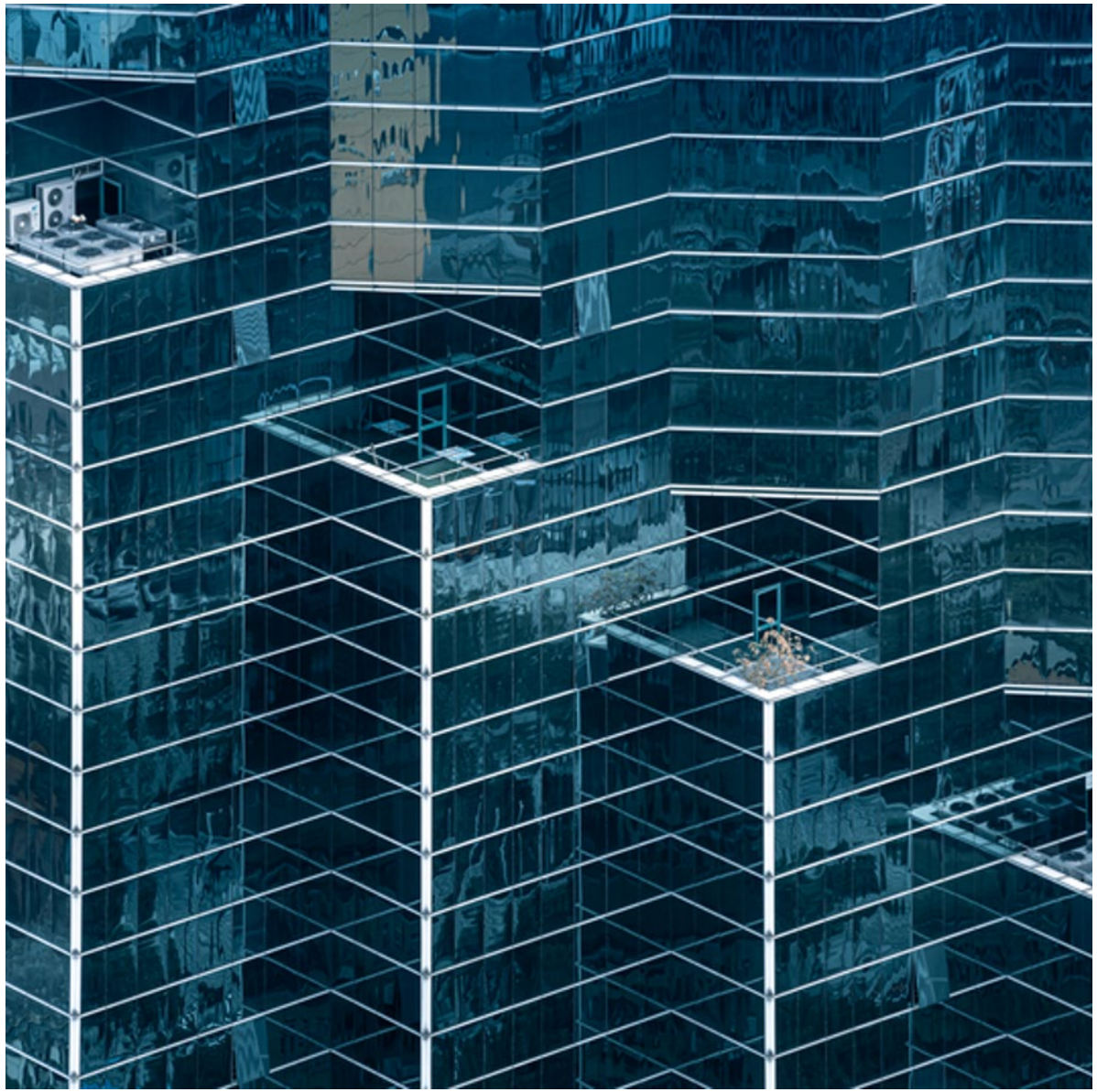
Supplier monitoring and contract terms for notification and audit rights reduce uncertainty before an incident.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Identity Hardening
Reducing the First Domino

- **Credential Abuse Leads In**
  Stolen credentials and vulnerability exploitation remain the leading ways attackers gain broad access without detection.
- **Phishing-Resistant MFA**
  Prioritize phishing-resistant MFA for privileged, remote, and vendor accounts to block common attack pathways.
- **Least Privilege & JIT Access**
  Reduce standing permissions with least-privilege and just-in-time elevation that attackers cannot easily exploit.
- **Monitor for Leaked Credentials**
  Watch for exposed credentials and unusual access, especially from vendor or unmanaged environments, to enable early warning.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Backups, Segmentation, & Recovery
Preserving Recovery Options

- **Immutable, Tested Backups**
  Most ransomware attacks target backup infrastructure, so backups should be tamper-proof and restored on a regular cadence.
- **3-2-1-1 Baseline**
  Keep three copies on two media types, one offsite, and one immutable or air-gapped copy that can survive compromise.
- **Segmentation Helps Limit Spread**
  Segmentation contains attacker movement, particularly from supplier access into core business systems.
- **Cloud & SaaS Coverage**
  Extend recovery planning to cloud and SaaS dependencies that traditional backup strategies can miss.



© 2026 Forvis Mazars, LLP. All rights reserved.

Supplier & Third-Party Risk

Reducing Downstream Exposure

Tiered Supplier Inventory

A ranked inventory of critical suppliers focuses monitoring and response where data and operations matter most.

Contract Language

Terms for notification, audit rights, subcontractor transparency, and security minimums help reduce ambiguity in a crisis.

Continuous Monitoring

Ongoing signals on critical vendors catch new exposure between annual or regular reviews.

Insurance Alignment

Align contract obligations with cyber insurance to help avoid coverage delays or denials during a claim.

Where This Breaks Down

Vendor Gaps Found Late

Discovering missing notification or cooperation terms mid-incident slows downstream decisions.

Coverage Mismatches

What you promised customers may cost more than insurance will pay, leaving you to cover the difference.

Unclear Ownership

When vendor reviews are a compliance checkbox rather than an owned program, no one knows who calls the vendor, briefs leadership, or notifies customers.

Legal Review Required

Confirm specific clauses with legal counsel before relying on them in negotiations.

© 2026 Forvis Mazars, LLP. All rights reserved.

Who You Must Tell & When

Clocks Measured in Hours

Banks: 36 Hours

Federal bank regulators expect notice within 36 hours of deciding an incident materially disrupts operations. Credit unions have 72 hours to tell the NCUA.

New York DFS: 72 Hours, 24 for a Payment

Licensed financial firms report incidents within 72 hours and any ransom payment within 24 hours, with a written explanation 30 days later.

Public Companies: 4 Business Days

Once an incident is judged material, the SEC expects a Form 8-K within four business days.

Before Any Payment: Sanctions Check

Paying a sanctioned group is a violation even if you did not know. Screen first, tell the FBI, and get your insurer's consent in writing.

Clocks Measured in Days

HIPAA: 60 Days

Ransomware that touches patient data is presumed a breach. Patients, HHS, and often the media must hear within 60 days of discovery.

State Laws: 30 to 60 Days

Every state has a notice law. California moved to a hard 30-day deadline in 2026, and many states also require notice to the attorney general.

Non-Bank Lenders: 30 Days

The FTC Safeguards Rule requires notice within 30 days when 500 or more consumers are affected.

Coming: CISA Reporting

A federal rule requiring 72-hour incident and 24-hour payment reports to CISA is expected to be finalized in late 2026. This is not legal advice; confirm deadlines with counsel.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Executive Tabletop Flow
Practicing High-Consequence Decisions

Realistic Trigger	Start from a supplier reporting data theft or an extortion demand, not a technical alert.
Key Decisions	Work data triage, legal privilege, communications, notifications, insurance, and law enforcement.
Parallel Response	Run containment and recovery alongside business decisions so both tracks move together.
After-Action	Capture lessons learned, contract updates, control remediation, and board reporting.

© 2026 Forvis Mazars, LLP. All rights reserved.

The First 24 Hours

What a Leader Does Before the Technical Answers Arrive

Slow down the decisions that cannot be undone. Speed up the calls that keep your options open.

First Hour

Get your incident lead, legal counsel, and insurer on one call. Do not pay, post, or email customers yet.

First 4 Hours

Decide who speaks for the company. Start a written timeline. Preserve evidence instead of wiping and rebuilding.

First 12 Hours

Confirm what the attackers actually have before reacting to what they claim. Brief the board chair or owner.

By 24 Hours

Know which notification clocks have started, who is calling key customers and suppliers, and what tomorrow's operating plan is.

© 2026 Forvis Mazars, LLP. All rights reserved.

Executive Tabletop Walkthrough
Communications, Notification, & Insurance

One Incident Narrative

Create a consistent narrative across legal, security, communications, and leadership.

Validate Attacker Claims

Use forensic evidence to confirm what data actually left before responding to threats.

Pre-Mapped Notifications

Map notification duties in advance by data type, jurisdiction, contract, and customer impact.

Early Insurance Coordination

Engage cyber insurers early, following policy terms, to preserve coverage and response resources.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Common Pitfalls
What Expands the Blast Radius

Underestimating Data Theft

Treating ransomware as only a restoration problem ignores stolen data and stakeholder consequences.

Vendor Gaps Found Late

Discovering missing vendor terms during an active incident increases uncertainty and delay.

Delaying Legal & Privacy

Waiting to involve legal or privacy until public pressure mounts narrows the available options.

Excluding Key Teams

Exercises without procurement, communications, or operations can slow decisions.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Executive Action Checklist
30/60/90 Days Without Boiling the Ocean

Make measurable progress across security, procurement, and operations.

First 30 Days

Identify critical suppliers and privileged access paths, and confirm incident and insurer contacts.

By 60 Days

Test backup restoration for priority systems and review key vendor contracts for notification and cooperation.

By 90 Days

Run an executive tabletop and convert the findings into a funded remediation plan.

Then Sustain

Assign named owners, track tested recovery objectives, and report progress to the board.

© 2026 Forvis Mazars, LLP. All rights reserved.

Five Questions to Ask Your IT Team
Answers You Can Check

- **If we lost every system today, how long until we are running again?**
  The answer should be a tested number, not an estimate. Ask when a full restore was last practiced.
- **Who can reset passwords or wipe devices, and does it take one person?**
  One administrator account with that power is the weak point the Stryker attackers used.
- **Which vendors can reach into our network or hold our customer data?**
  If that list does not exist, building it is the first project.
- **How would we know if someone were inside right now?**
  Attackers often sit for weeks. Ask who is watching, and during which hours.
- **Who do we call in the first hour, and is the list printed?**
  Maintain accessible contact information for the insurer, counsel, incident responders, and applicable regulatory contacts.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Key Takeaways

Modern extortion is a business problem that reaches every department.

Expect Multifront Attacks

Supplier compromise and multi-party extortion can amplify the financial, legal, and operational impact of a single event.

Invest in High-Leverage Controls

Identity hardening, immutable backups, segmentation, and strong contracts can help reduce losses.

Coordinate the Response

Security, legal, communications, procurement, and insurance should move together, supported by tested tabletops.

Practice Executive Decisions

Practice the calls only leaders can make: whether to pay, what to say publicly, and when to notify regulators and customers.

© 2026 Forvis Mazars, LLP. All rights reserved.



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.



Don’t Miss the Next Session of the

2026 Cybersecurity Virtual Symposium

Healthcare Cyber & Privacy: Moving Beyond HIPAA Baselines

Today at 2:00 p.m. - 3:00 p.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Paul Truitt
Principal
215.913.9968
paul.truitt@us.forvismazars.com

Justin Lance
Senior Manager
704.367.7047
justin.lance@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.