

Manufacturing Modernization
Cybersecurity as a Business Imperative

October 2026

forvis mazars

Today's Presenters
With a Focus on Cybersecurity & Third-Party Risk Management



Korey Barrette
Director, IT Risk & Compliance · vCISO Lead korey.barrette@us.forvismazars.com



Mareena Bowen
Manager, IT Risk & Compliance · TPRM Lead mareena.bowen@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Today's Session
Building on the 2026 Modernization Series



Digital Transformation

- April 2026
- Cloud, ERP, and AI adoption accelerate growth and widen the attack surface



Workforce Transformation

- July 2026
- Connected workers and rapid change introduce human risk and new access points



Supply Chain

- August 2026
- Reshoring and new suppliers add vendors, geographies, and third-party exposure

TODAY



Cybersecurity

- October 2026
- Cyber readiness can help organizations pursue more resilient, defensible modernization.

Sessions 1-3 are available on demand - ask your Forvis Mazars contact or the moderator for the recording links.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Learning Objectives

Upon completion, participants will be able to:

1

Discuss the importance of cyber readiness as a pillar of digital transformation.

2

Recognize the cybersecurity considerations for integrating AI, automation, and third-party technologies into business operations.

3

Identify what security operations teams should do to prepare for threats.

© 2026 Forvis Mazars, LLP. All rights reserved.

01

Cybersecurity as a Pillar of Digital Transformation



The Business Case
Why Cybersecurity Is Imperative

$4.99M average cost of a data breach (global, all industries)

Source: breach-cost figure is a global, cross-industry average. Strategic-priority point: C-Suite Barometer 2026 (U.S.), FORsights, Forvis Mazars.

As manufacturers move to the cloud and adopt AI and automation, connectivity expands cyber risk, particularly through third-party relationships.

A cyber incident can halt production and affect uptime, safety, revenue, and compliance.

Transforming IT and technology now ranks as the #1 strategic priority for U.S. executives—making cybersecurity core to the growth agenda.

© 2026 Forvis Mazars, LLP. All rights reserved.

Prioritizing Cybersecurity
Governance & Remediation

IT and cybersecurity issues often have governance roots. Unclear accountability and gaps in policy, configuration, or follow-through should be addressed.



The Pattern

- Business units make separate technology requests
- IT carries a long list of projects with overlapping dependencies
- Cyber, infrastructure, and data decisions stay siloed
- Vendors end up influencing the roadmap



The Risk

- Security work competes with new systems for attention
- Findings are reviewed one request at a time, not as a portfolio
- Leadership lacks context to make informed trade-offs
- Modernization outpaces the ability to govern it safely



The Fix

- Build a shared current-state view of applications, data, security, and vendors
- Turn the project list into a decision portfolio
- Identify applicable customer contract clauses and confirm their scope.
- Create governance with a regular review cadence
- Name the executive who owns and reviews the risk

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

02

Third-Party Risk Management (TPRM) & Artificial Intelligence (AI)



Third-Party & Nth-Party Risk

Outsourcing the Work Does Not Eliminate the Risk



You	Third Party	Fourth Party	Nth Party
Your organization — the data, systems, and operations you own	The vendor you contract with directly	The subcontractor your vendor relies on	Cloud hosts, processors, and AI models deeper in the chain

Contractual reach and visibility decrease with every step outward

Visibility and assurance often decline farther down the chain. Focus deeper mapping on critical services, concentration, data, and access.

Where to look one level deeper

- Shared cloud platforms, processors, MSPs, and AI model dependencies
- Concentration risk: several critical vendors resting on one provider
- Subservice organizations named in SOC reports for critical services
- The full AI chain, not only the model provider you contracted with

© 2026 Forvis Mazars, LLP. All rights reserved.

The Vendor Management Lifecycle
From Onboarding Through Offboarding

Vendor risk management should continue beyond onboarding. A vendor reviewed once at signature can drift for years before anyone looks again.



Onboard

- Set the vendor tier before the contract is signed
- Collect SOC 2, ISO 27001, or penetration test evidence up front
- Negotiate security terms, breach notification windows, and right to audit
- Name the internal business owner accountable for the relationship



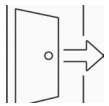
Assess

- Map questionnaire items to NIST CSF or ISO 27001 controls
- Review applicable report details, including scope, identified exceptions, and relevant subservice organizations.
- Test claims against evidence, not self-attestations alone
- Document accepted risks with an owner and expiration date.



Monitor

- Re-assess on the tier's cadence, not when someone remembers
- Track continuous signals: breach news, security ratings, financial health, etc.
- Re-trigger review on scope, subprocessor, or AI model changes



Offboard

- Trigger exit on contract end, replacement, or termination for cause
- Revoke access: accounts, VPN, API keys, badges, and integrations
- Confirm data return or destruction in writing
- Close out final invoices and capture lessons learned

© 2026 Forvis Mazars, LLP. All rights reserved.

Vendor Tiering
Focus Effort Where Risk Concentrates

Tier 1 – High Risk

What It Is

Touches production, OT, or regulated data – an outage stops the line

What It Deserves

Full assessment, annual review, security terms in the contract, and an exit plan

Tier 2 – Moderate Risk

What It Is

Supports operations or holds sensitive data – disruption is absorbable

What It Deserves

Targeted review of the controls that matter to that service

Tier 3 – Low Risk

What It Is

No sensitive data or system access – commodity services

What It Deserves

Consider self-attestation or other streamlined diligence based on the organization's risk criteria.

Set the tier on evidence, not spend:

- Score production impact, access, data, substitutability, and concentration; regulated or sensitive data can increase the tier - apply your own risk criteria
- A low-spend vendor with deep access can still be Tier 1; re-tier when scope changes
- Three tiers is the common baseline; mature or regulated organizations often have four or five tiers

© 2026 Forvis Mazars, LLP. All rights reserved.

From Findings to Action
What to Do With What You Find

Triage

Prioritize using technical severity, exploitability, exposure, business impact, compensating controls and remediation feasibility.

Own

Give every finding a named internal owner, a vendor counterpart, a target date and a defined escalation threshold.

Remediate

Agree on a remediation plan with the vendor and move material items into contract or SLA language.

Escalate

Define the threshold that triggers leadership review, renegotiation, or exit.

Report

Roll findings into one risk view tied to uptime, revenue, and compliance exposure.

© 2026 Forvis Mazars, LLP. All rights reserved.

Adopting AI Responsibly
Two Questions Leaders Face With AI



External Risk

How might AI affect the threats directed at us?

- Which of our exposures become easier to find, exploit or automate against? Assess this for our own environment rather than assuming a market-wide figure.



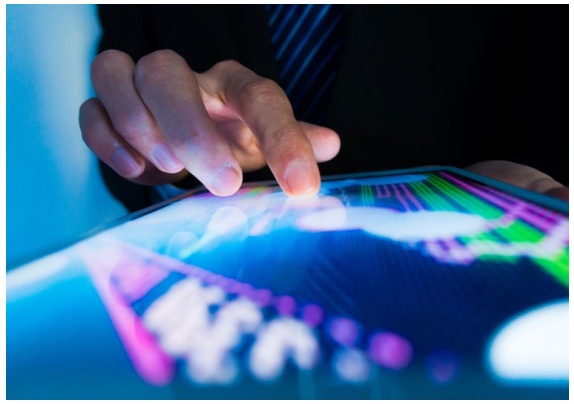
Internal Risk

What new exposure will we create by embedding AI?

- AI systems may be able to retrieve sensitive data, connect to critical systems, and act through user or agent permissions; some of these AI tools may be managed by a third party.

© 2026 Forvis Mazars, LLP. All rights reserved.

Adopting AI Responsibly
Actions to Consider Now



Inventory AI-enabled workflows, owners, and permissions

Reassess after any material change to model, scope, or permissions



Limit agent authority: least privilege and tool/action allowlists

Require human approval for high-impact actions



Expand security testing: prompt manipulation and untrusted content

Set data retention and training-use rules with each provider



Update incident procedures to capture prompts and retrieved content

Log agent actions and name an incident owner for AI systems

Source: AI Cybersecurity Risks — Practical Guidance for Leaders, Forvis Mazars.

© 2026 Forvis Mazars, LLP. All rights reserved.

03

Frameworks That Make the Program Repeatable



Frameworks
Governing, Assessing, & Demonstrating Assurance

Third-party risk frameworks are most useful when aligned with the organization's applicable obligations. Start from the customer flow-down clauses and other binding requirements that apply to you, then use these to answer who decides, what good looks like, and how it can be proven.



COBIT

- Govern enterprise information and technology
- Helps structure decision rights and governance and management objectives
- Tailor it to the organization



NIST CSF 2.0

- Describe cybersecurity outcomes
- Six functions: Govern, Identify, Protect, Detect, Respond, Recover
- Use profiles to describe current and target outcomes
- It is not a vendor certificate



ISO/IEC 27001

- Requirements for an information security management system (ISMS)
- If a supplier claims certification, ask for the certificate and scope
- Compare the covered organization and services with the service and data involved

NIST SP 800-161 Rev. 1 — direct C-SCRM reference: use as additional supply-chain guidance for supplier, product and service risk, not as a vendor certificate.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Frameworks for AI
Where AI Assurance Is Heading

NIST AI RMF 1.0

What It Is

Voluntary AI risk-management framework; NIST says the framework is being revised. Use it to structure risk work across AI design, development, use, and evaluation.

Where It Stands

Use it now to structure AI risk work

ISO/IEC 42001:2023

What It Is

Published AI management-system standard. Organizations may seek independent certification; ISO itself does not certify organizations.

Where It Stands

Independent certification is available through accredited bodies

AIUC-1

What It Is

Emerging AI-agent security, safety and reliability standard with a certification program. Check current version, scope, assessor, test results and certificate status.

Where It Stands

One emerging, optional assurance option where agent behavior is material - not a market baseline. Verify version and product scope; certification does not eliminate the buyer's own risk assessment

Whatever the framework, ask every AI vendor the same three questions:

- Which model, hosting, subprocessor and data locations are in the service chain? What data is retained or used for training?
- Which tools, systems and data can the AI access? How are permissions scoped, logged and revoked? Which actions require human approval?
- How are prompt injection, untrusted content, data leakage, unsafe tool calls, and service changes tested and handled?

Ask the vendors you signed — and ask about the vendors behind them.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Make It Repeatable
Without Duplicating the Work

In Practice

- Build one internal control set and map it to applicable frameworks, such as COBIT, NIST CSF, and ISO/IEC 27001.
- Let the vendor tier decide which controls you test and how deeply
- Reuse current, relevant evidence; validate scope and exceptions; request targeted supplements only for gaps
- Add AI-specific questions for any vendor embedding models or agents
- Track exceptions centrally so leadership can see aggregate exposure
- Re-map annually; AI standards in particular are moving quickly

Map Once & Reuse

- **Build 1 control set.** Map applicable controls to each relevant framework.
- **Set 3–5 vendor tiers.** Let the tier decide how deep each assessment goes.

Map once so one piece of evidence can answer several frameworks.

Reference: The Secure Controls Framework® (SCF).

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

04

What Security Operations Should Do to Prepare for Threats



From Supplier Risk to the Plant Floor
Carrying the Risk Forward

Access

Third parties and AI tools hold credentials, remote connections, and data paths into the environment you operate.

Crossing

That access does not stop at IT. Supplier connections and integrations reach toward the plant floor and the OT boundary.

Exposure

Legacy endpoints, OT, and connected assets are hard to patch, so inherited risk lands where recovery is hardest.

Detection

Security operations has to see vendor and AI activity as monitored, logged events, not as trusted traffic.

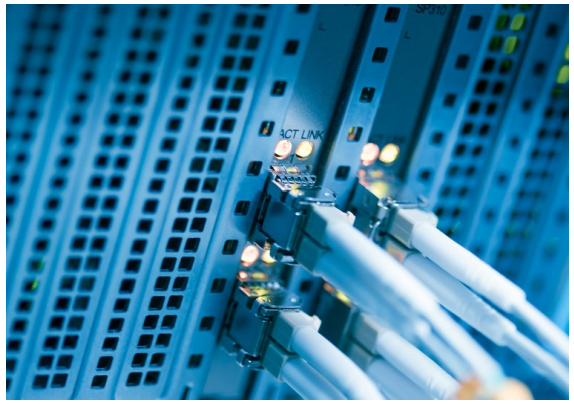
Response

Tiers, owners, and escalation thresholds from the vendor program become the playbook when production is at stake.

© 2026 Forvis Mazars, LLP. All rights reserved.

The Threat Landscape Beyond Third-Party & AI Risks

Where Manufacturing Is Exposed



Ransomware

Ransomware may encrypt systems, disrupt production, and contribute to downtime and recovery costs.



Legacy & OT Systems

Some legacy endpoints and operational technology may be difficult to patch and can complicate recovery.



IoT & Connected Assets

Sensors and connected equipment expand the attack surface and can disrupt operations.



IT/OT Integration

As factories connect, IT threats now reach the plant floor and the supply chain.

© 2026 Forvis Mazars, LLP. All rights reserved.

Be Ready
From Detection to Response

Prepare, Detect, & Respond

- Map critical assets and dependencies across IT and OT
- Consider appropriate IT and OT segmentation and layered remote-access controls based on the environment's risk and operational requirements
- For legacy systems that cannot be patched, apply named compensating controls and assign a residual-risk owner
- Monitor OT networks for anomalies with specialized tools
- Maintain tested offline, immutable backups of PLC logic, HMI projects and device configurations, validated with engineering and safety owners
- Test incident response with OT-specific scenarios

Measure Resilience

Mean time to detect (MTTD):

Time from event start (first malicious activity on IT/OT) to confirmed detection. Report consistently by incident type and severity.

Mean time to contain (MTTC) or
Mean time to respond / recover (MTTR):

Time from detection to a defined containment or recovery endpoint, with the operating impact that endpoint implies.

Pair cyber response measures with plant outcomes: time to safe state, service/line downtime, recovery time, and integrity of restoration.

© 2026 Forvis Mazars, LLP. All rights reserved.

Put It Into Practice
Actions to Take Now

Govern
Name the accountable executive. Report exposure, trend, and the decision you need.

Prioritize
Bring open security findings into the same portfolio as growth and modernization initiatives.

Protect
Map critical assets, segment IT and OT, and test incident response with OT-specific scenarios.

Manage Vendors
Tier vendors by risk and build Nth-party visibility for your most critical services.

Adopt AI Safely
Inventory AI-enabled workflows, limit agent authority, and expand security testing.

© 2026 Forvis Mazars, LLP. All rights reserved.

Key Takeaways

- Cyber risk belongs in modernization governance.
- Tier and monitor suppliers - including critical Nth-party dependencies.
- Bound AI permissions and test changes.
- Rehearse OT-specific response.
- Choose one owner and one action for the next 30 days.

Cybersecurity is no longer just an IT issue; it is a business imperative.

© 2026 Forvis Mazars, LLP. All rights reserved.

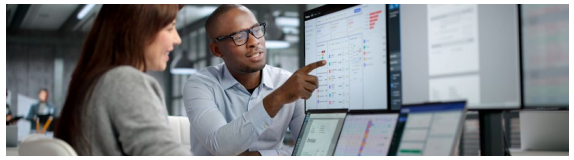
Questions?

Let’s Discuss What Cyber Readiness Looks Like for Your Operations.



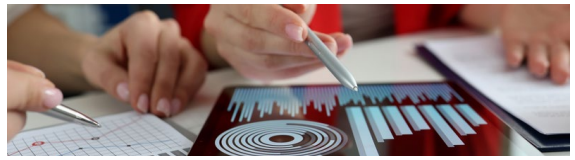
How Forvis Mazars Can Help
Cybersecurity Consulting

An on-demand model brings virtual CIO and CISO advisory together with remediation support and third-party risk management to help connect business priorities and technical findings with defined actions.



vCIO

Connect technology planning to business priorities. Develop roadmaps, governance practices, resource priorities, and executive reporting.



vCISO

Strengthen cybersecurity governance and program oversight. Clarify security priorities, support readiness, and translate technical matters.



Remediation

Move findings toward sustainable resolution. Prioritize gaps, define action plans, support improvements, and report progress.



TPRM

Manage vendor and supply chain exposure. Assess critical third parties, set diligence standards, and monitor ongoing risk.

© 2026 Forvis Mazars, LLP. All rights reserved.

Contact

Forvis Mazars

Korey Barrette
Director, IT Risk & Compliance
korey.barrette@us.forvismazars.com

Mareena Bowen
Manager, IT Risk & Compliance
mareena.bowen@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.