Third-Party and Vendor Cyber Risk: Your Weakest Link Isn't IT

PRESENTED By

Adam Wisnieski

June 10, 2026

SLG UNIVERSITY

Your Instructor

Adam Wisnieski
Partner

Agenda

1. **Introduction**
2. **Why Third Parties Introduce Risk**
3. **Overwhelmed with Reviews? Let's Simplify!**
4. **Wrap Up**

Learning Objective

By the end of this course, you should be able to:

- Identify third-party cyber risks by evaluating vendor access, data sensitivity, and contractual controls.

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

MGO.

Introduction

SLG UNIVERSITY | MGO.

The Invisible Infrastructure

Imagine your government building has the world's most secure vault door: an IT firewall. To keep the building running, you give keys to the janitor, elevator repair crew, and document shredding service. If one of them loses a key, the vault door doesn't matter.

Traditional Approach

We focus on the **front door** or direct hacks while the **loading dock** for vendors is left wide open.

Mindshift

Procurement isn't just buying a service. It's importing risk. Every contract signed is a potential bridge into your network.

Why You're in the Cybersecurity Conversation

Cyber risk is created long before an incident occurs.

The Goal

We want to move cybersecurity from a technical **IT issue** to a core fiduciary responsibility.

We'll talk about how to spot a risky vendor before you sign them and how to protect your organization when things go wrong.

What This Session Will and Won't Do

Today's focus

Real incidents affecting governments

Practical, defensible approaches

Finance and procurement actions

Technical security configurations

Blaming IT

Poll 1: Cyber Risk Exposure

Which action most directly increases your organization’s cyber risk exposure?

- IT strengthens the firewall controls
- Procurement selects a vendor without evaluating risk
- Security team encrypts sensitive data and emails
- IT updates system patches regularly

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

mgo.

MGO.

Why Third Parties Introduce Risk

SLG UNIVERSITY | MGO.

Most cyber incidents impacting governments or other organizations start with a third party.

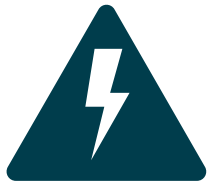
The Reality of Modern Government Vendors When Thinking of Cyber Risks

SaaS and Cloud Platforms

Managed Service Providers (MSPs)

Payroll, HR, Billing, and Utilities

Permitted and Case Management Systems



Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO.

Why Attackers Target Vendors

Vendors are force multipliers.

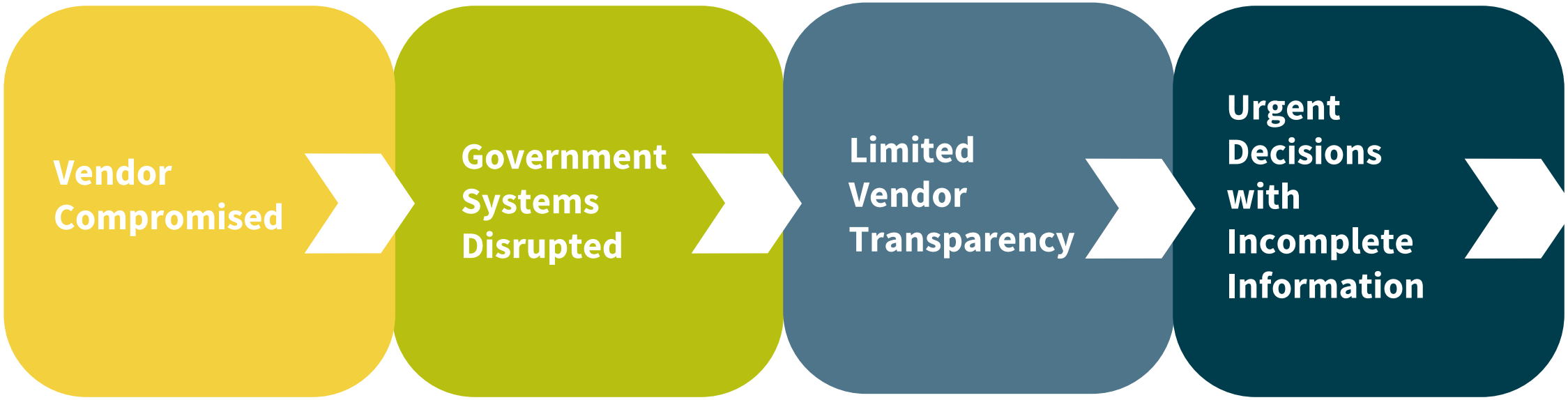
- One breach equals access to many clients
- Broad system access
- Often weaker security than governments they serve

The Hidden Risk: Inherited Security

You inherit your vendor's weaknesses.

- Poor access controls
- Unencrypted data
- Weak backups
- Slow breach detection

How Vendor Incidents Typically Unfold and Impact Agencies



Poll 2: Third-Party Vendors

Why do attackers often target third-party vendors instead of government agencies directly?

- Governments lack cybersecurity defenses
- Vendor incidents create less public impact
- Vendors provide force-multiplier access
- Vendors rarely store client-sensitive data

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

mgo.


MGO.
Overwhelmed with Reviews? Let's Simplify!
SLG UNIVERSITY
MGO.

But we can’t do a deep-dive review of every vendor … it’s true and not required. Let’s see how.

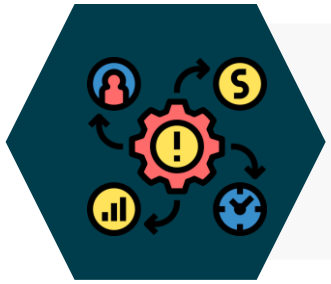
Right-Sizing Vendor Risk

Risk depends on the following.

Data Sensitivity

System Criticality

Access Level



Operational Impact

Why Include Non-IT Vendors?

It’s not about the vendor’s product: It’s about the vendor’s access. Here are some hidden risks.

1

Remote Access Tunnels

This is your HVAC and building automation.

2

Service PII Handlers

These are your legal and professional services.

3

Physical Access to Hardware

These are your janitorial and maintenance teams.

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO.

Case Study #1: Engineering Firm Email Compromise

Scenario

- A local government engages a third-party engineering firm to support a multi-year program.

Vendor

- Receives citizen and employee data.
- Exchanges documents by email and shared folders.
- Uses its own systems and cloud storage.
- Is not classified as an IT vendor.

Several months into the engagement, the vendor experiences a **business email compromise (BEC) incident**.

How Did this Unfold?

- Attacker accessed vendor's email account.
- Observed invoicing and payment cycles.
- Sent a spoofed message requesting a banking change.
- Payment was rerouted to an attacker-controlled account.
- Fraud was discovered weeks later during reconciliation.

Vendor-Side Issues

- No multi-factor authentication (MFA) on emails.
- Weak password controls.
- Lack of employee phishing training.
- Minimal incident detection capabilities.
- Attackers gained access to vendor email accounts and initiated conversations.

Agency-Side Issues

- Vendor assumed **low cyber risk** because it was non-IT.
- No cybersecurity language in contract.
- No requirement for breach notification.
- No verification procedures for payment or banking changes.

Key insight: This vendor never touched any internal systems. Only emails and documents.

The Impacts

Financial	▪ Six-figure payment diverted, with unrecoverable funds and loss not fully insured ▪ Required budget reallocation
Operational	▪ Delayed project milestones ▪ Investigation and remediation costs ▪ Manual validation of all vendor payments
Reputational and Governance	▪ Questions from leadership and council ▪ Audit and oversight review ▪ Reputational damage despite no **system breach**

So why did this become a finance and procurement issue?

- Payment controls failed under social engineering.
- Contract did not address cyber or fraud responsibility.
- Insurance exclusions for fraud limited recovery.
- Procurement had no leverage post-contract.

This incident bypassed IT entirely and hit finance, procurement, and operations directly.

Concentration Risk

In government, especially at the state and local level, we often rely on a very small pool of niche providers.

Concentration risk means we're not just exposed to one vendor. It means we're exposed to the same vendor across the board.

- Do we know which vendors we share with peer governments?
- Do we understand which outages would cripple revenue or service delivery?
- And have we planned for regional disruption, not just local incidents?

Poll 3: Vendor’s Cyber Risk Level

Which factor most strongly determines a vendor’s cyber risk level?

- Vendor’s access to sensitive data
- Total dollar value of contract
- Number of years vendor has worked
- Whether vendor is classified as an IT provider

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

MGO

1 **Regional payroll SaaS provider hit by ransomware**

2 **Multiple cities and counties effected**

3 **Payroll delayed for weeks**

Case Study #2: Payroll Provider Ransomware

Scenario

Poll questions: Join MGOcpa.cnf.io

mgo.

Impact and Questions

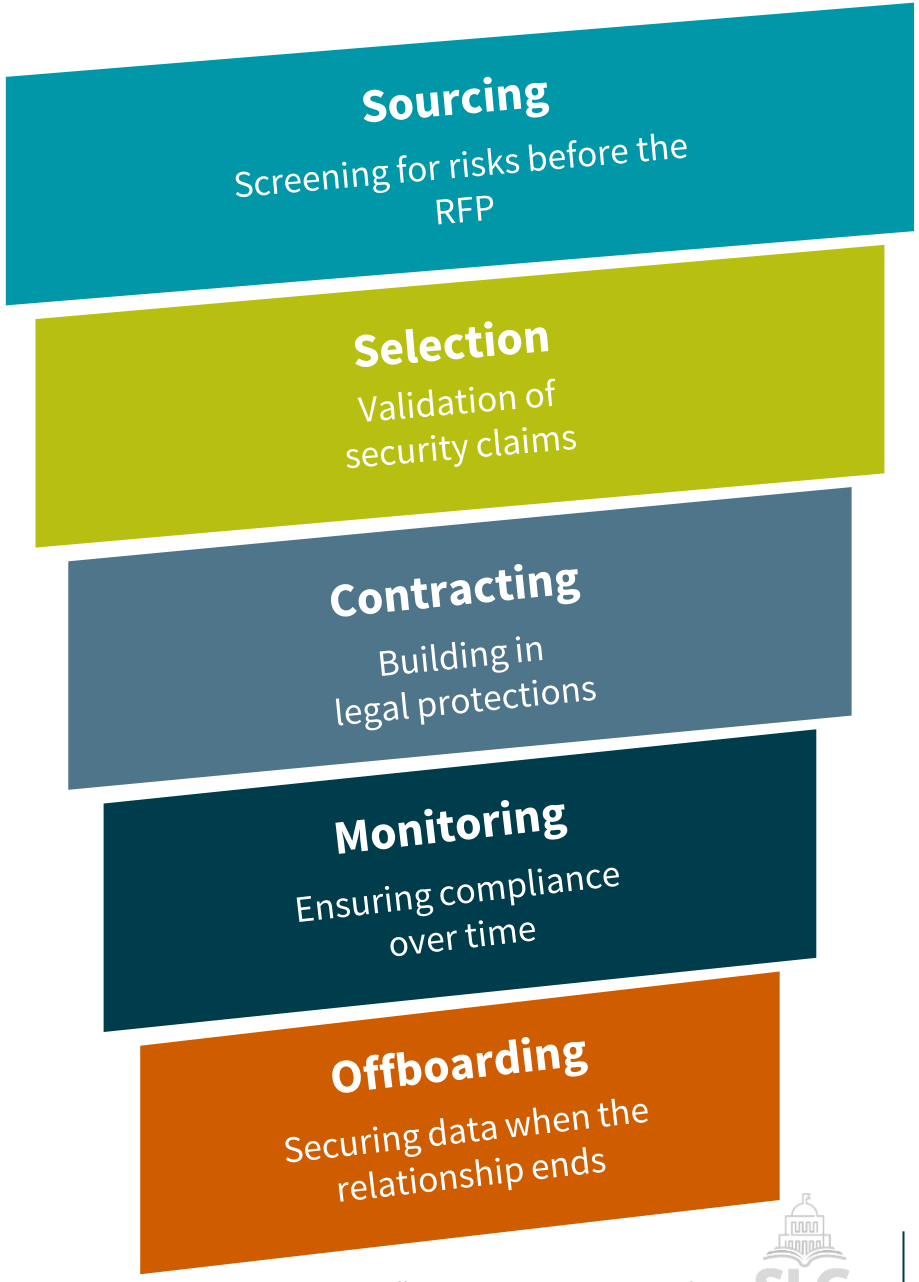
- Employees unpaid or paid late
- Emergency manual processes
- Overtime and consulting costs
- Public pressure and leadership scrutiny

1. What did the contract say about incidents?
2. Who pays for recovery costs?
3. Did the vendor notify promptly?
4. Was insurance applicable?

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO.

An Overview of the Third-Party Risk Management (TPRM) Life Cycle



Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

Sourcing

Screening the risk before the RFP.

Reasonable does not equal perfect

Scaled to risk

Consistent across vendors

Defensible to auditors and leadership

Selection: Validating Security Claims

What should you ask vendors?

01

How is our data being protected?

How

02

Who can access our systems?

Who

03

How fast will you notify us of an incident?

How

04

Who pays if something goes wrong?

Who

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

Contracting: Building in Legal Protections

This isn't about being adversarial.

It's about protecting the public interest and ensuring that cyber risk is allocated knowingly and fairly before something goes wrong.

1 **Right to Audit**

You must verify, not just trust.

2 **Notification Window**

24 – 48 hours for incident reporting and it's mandated.

3 **Data Ownership**

Explicitly state the data belongs to the government, not the vendor.

4 **Liability Caps**

Ensure indemnity isn't capped at just **contract value.**

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

Monitoring

Ensuring compliance over time.

Document

Document what you check. Defensibility matters as much as action.

Focus

Focus on high-risk vendors. Not every vendor needs ongoing review.

Confirm

Confirm incident readiness. Notification timelines still realistic.

Watch

Watch for material changes: ownership, systems, access, and data scope.

Verify

Verify, don’t assume. Security and risk change over time.

Keep

Keep it lightweight and periodic. Annual or risk-triggered reviews.

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

Offboarding

Securing data when the relationship ends.

Confirm

Confirm access is terminated: systems, accounts, and credentials.

Secure

Secure government data: return, deletion, or certified destruction.

Validate

Validate residual risk: backups, logs, and retained copies.

Capture

Capture lessons learned: inform future sourcing and contracts.

Close

Close paperwork: written attestations and documentation.

Revoke

Revoke integrations: APIs, network connections, and remote access.

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

MGO

Poll 4: Greatest Leverage

When does a government agency have the greatest leverage to manage third-party cyber risk?

- During annual vendor performance reviews
- When the vendor relationship ends
- During contract negotiation, before signing
- After a vendor incident occurs

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

MGO.

MGO.

Wrap Up

SLG UNIVERSITY | MGO.

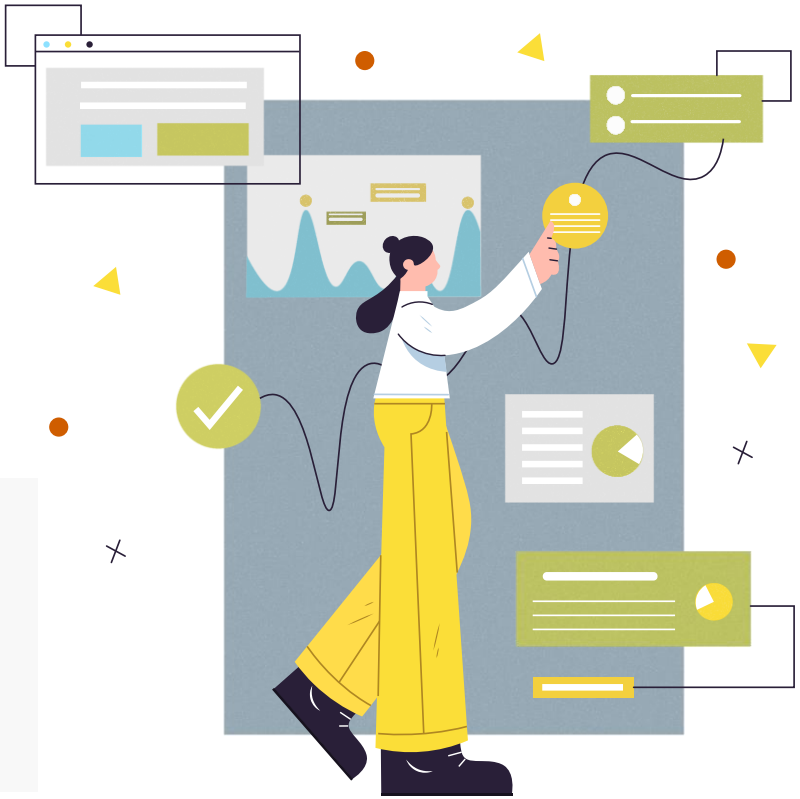
Take Away Plan

Map Your Crown Jewels

Identify the top five vendors who, if breached, would cause a total work stoppage.

The One-Question Audit

Ask your top vendors, “When was the last time a third-party audited your security, and can I see the results?”



Cross-Department Task Force

Procurement, finance, and IT should meet monthly, not just when a contract is up for renewal.

Review Insurance

Check your own cyber liability policy to see if it covers **contingent business interruption** caused by a vendor.

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY | MGO

Final Thoughts

Safety Codes

You wouldn’t hire a construction firm that doesn’t follow safety codes. You shouldn’t hire a vendor that doesn’t follow digital safety codes.

Choose Wisely

Your IT team builds the walls, but as procurement and finance officials, you’re the ones who decide who get the key. **Choose wisely**.

ANY QUESTIONS?

Poll questions: Join MGOcpa.cnf.io

SLG UNIVERSITY

MGO.