VENDOR BREACH SURVIVAL CHECKLIST

CYBERCRIME IS REAL. YOUR VENDORS ARE THE DOOR.

DON'T BE THE NEXT VICTIM

1. Why This Checklist Exists

Use this checklist so you're not blind when a vendor, cloud tool, or service your business relies on gets hacked.

- You understand that most modern attacks can reach you through vendors and SaaS tools.
- You want a simple, written plan for "what we do when a vendor gets breached."
- You will keep this document printed and accessible for yourself and your IT / MSP.

2. Step One – Map Your Critical Vendors ("Touch Points")

Goal: Know which vendors can actually hurt you if they're breached.

2.1 Make the list

List every external vendor / system that touches customer, staff, or sensitive business data.

For each, fill in a row like this:

- Vendor / Service: _____
- What we use it for: _____
- Data they hold or process for us (tick or mark in Word as needed):
  - Customer names / emails
  - Payment or billing data
  - Payroll / HR / salary data
  - Health / student / confidential records
  - Legal or contract documents
  - Internal files / IP
  - Other: _____
- How critical is this vendor to operations?
  - 5 – Can't operate without it
  - 4 – Heavy disruption if lost
  - 3 – Annoying but survivable
  - 2 – Minor impact
  - 1 – Barely used

2.2 Prioritize the top risks

- Highlight your top 10–20 most critical vendors.
- Mark which of these hold your highest-sensitivity data (payroll, health, legal, student, etc.).

3. Step Two – Assign Ownership and Decision Makers

Goal: When a vendor gets hit, there is no confusion about "who decides what."

For each high-risk vendor:

- Vendor / Service: _____
  - Business owner (who uses it day to day): _____
  - Technical owner (internal IT or MSP contact): _____
  - Final decision maker if there's a breach (name / role): _____

Global ownership:

- Assign one person who owns overall vendor risk (even if security is not their full-time job).
- Make sure this person knows they are responsible for triggering this checklist during a vendor incident.

4. Step Three – First 24 Hours After a Vendor Breach

Goal: Have a written, repeatable playbook for the first 24 hours when a vendor you use shows up in a breach or high-risk vulnerability alert.

4.1 Confirm and scope the incident

When you see a credible alert (from SMOKE, news, or the vendor):

- Capture the source of the alert (email, SMOKE notification, news link, etc.).
- Confirm what is being claimed: data theft, ransomware, critical vulnerability, outage, etc.
- Identify which of your systems and data might be involved.

Write down:

- Vendor name: _____
- Nature of incident (breach / ransomware / critical vulnerability): _____
- Date / time we became aware: _____

4.2 Immediate technical actions (with IT / MSP)

With your IT team or MSP:

- Review any access this vendor has to your systems (VPN, API keys, SSO, admin accounts).
- Decide if you need to temporarily limit or block access until more is known.
- Rotate relevant passwords, API tokens, and shared credentials.
- Enable extra verification where possible (MFA, IP restrictions, extra approvals).

- Start basic logging and evidence capture (screenshots, emails, vendor notices).

Notes / actions taken:

4.3 Communication in the first 24 hours

Internally:

- Notify key leadership (owner, operations, finance, HR).
- Notify the technical owner and business owner for that vendor.
- Tell staff not to make changes on their own without instructions (to avoid destroying evidence or creating confusion).

Externally (if needed):

- Check any legal or regulatory obligations for your sector and location.
- Prepare a short holding statement for customers, for example: “We are aware of a security incident involving one of our vendors. We are investigating any impact to your data and systems and will update you as soon as we have confirmed details.”

5. Step Four – Shorten the "Blind Window" with Continuous Monitoring

Goal: Stop relying on luck and vendor marketing slides; use ongoing signals instead.

Before anything happens:

- Maintain a single list of critical vendors (touch points).
- Know which ones hold your most sensitive data.
- Keep a simple, written 24-hour playbook (this document).

For ongoing visibility:

- Ensure you receive alerts when there are major vulnerabilities, breaches, or ransomware activity affecting tools like the ones you use.
- Make sure those alerts are tied to your actual vendor list, not random companies.
- Require that alerts be written in plain English with concrete actions for your IT / MSP.

How SMOKE by INVISIQ fits:

- Upload or keep your vendor / touch-point list in SMOKE.
- Use SMOKE to watch for "smoke" around those vendors – breaches, high-risk vulnerabilities, and public indicators of trouble – and send clear guidance before attackers reach you.
- Update your touch-point list whenever you add or remove a major vendor or cloud system.

6. One-Page Quick Reference (Print This)

When a vendor we use appears in a breach or high-risk alert:

1. Pause and document.
    - Save the alert or notice.
    - Write down the date and time we found out.
2. Identify the vendor and what they hold.
    - Check the vendor list: what data do they store for us?
    - How critical are they (1–5)?
3. Talk to the right people.
    - Notify the assigned vendor owner.
    - Notify IT / MSP.
    - Notify leadership (owner / director).
4. Lock down what you control.
    - Consider temporarily limiting access from/to that vendor.
    - Rotate passwords, API keys, and integration tokens.
    - Enable any extra verification you can (MFA, approvals, IP limits).
5. Follow SMOKE's guidance (if enabled).
    - Review the SMOKE alert for this vendor.
    - Execute the specific actions recommended for the next 24 hours.
    - Record what was done and by whom.
6. Decide on communications.
    - Check if you're required to notify regulators or authorities.
    - Prepare a clear, honest update for customers if their data might be involved.

This checklist is not about turning you into a security expert.
It's about making sure that when a vendor gets hacked, you are:

- not blind,
- not guessing, and
- not finding out from the news before you hear it from your own systems.

Keep this document where you can find it quickly — and keep SMOKE by INVISIQ watching the vendors you depend on, so your first warning is an early alert, not a crisis.