Could a **supplier open the door** to your business?

HOW TO REDUCE SUPPLY CHAIN RISK, CONTROL SHADOW IT AND COLLABORATE SAFELY WITH CUSTOMERS, VENDORS AND PARTNERS.

A CLEAR, PRACTICAL CHECKLIST
FOR NORTH WEST SMES

Your security boundary no longer stops at your front door.

Modern SMEs share systems, files and data with cloud providers, software vendors, accountants, HR platforms, resellers, customers and contractors. Every connection creates value, but every connection also creates a route that needs managing.

A supply chain incident can begin elsewhere

A trusted third party can be compromised, exposing shared information, credentials or connected systems. The supplier may be the weak point, but the impact lands with your business and your customers.

Shadow IT makes that web harder to see

Shadow IT is any app, device, software or service used for work without explicit approval from the people responsible for IT and security. It often starts with good intentions: somebody finds a quicker way to schedule the event, share a file or collaborate with a partner. The risk is that nobody has checked how the tool stroes data, controls access or responds to the incident.

Key thought...
If nobody knows a tool is in use, nobody can secure it

Four relationships.
Four places to ask better questions.

Software and cloud vendors

Do they handle sensitive data? Is the service approved? Who reviewes access, security updates and contract changes?

Distributors and resellers

What information can they see? Are shared portals and credentials controlled? Are content and data-sharing rules clear?

Customers and end users

Are staff following agreed methods for file sharing, remote access and identity checks when helping customers?

Specialist partners

HR, payroll, legal. finance and marketing partners may process valuable data. Are responsibilities and escalation routes documented?

The common thread...

External collaboration isn't the problem. Unclear ownership, unapproved tools, excessive access and weak communication are the problem.

Five controls
that make the biggest difference.

Keep an approved-tools list

Make the safe choice obvious. Tell employees and partners which tools are approved and where to request alternatives.

Map your critical suppliers

Record which suppliers hold data, connect to systems or support essential services. Assign an internal owner.

Set minimum security expectations

Build security, access, confidentiality, incident notification and offboarding requirements into supplier conversations and contracts.

Train internal and external teams

Explain the risks of unapproved tools, shared credentials and unexpected links or attachments. Make reporting simple.

Review access and tools regularly

Remove access that's no longer needed, check which tools are actually in use and revisit higher-risk relationships more often.

Security works best when everyone knows what "approved" looks like.

Could you answer “yes” to these questions?

- [ ] We know which third parties can access our systems or sensitive information.
- [ ] Employees and partners know which apps and tools are approved.
- [ ] There is a simple route for requesting a new tool or reporting an unapproved one.
- [ ] Critical suppliers have a named internal owner and a documented purpose.
- [ ] Access is reviewed and removed when people, roles or contracts change.
- [ ] Suppliers know how quickly to tell us about a suspected security incident.
- [ ] Staff know to pause before clicking unexpected links or attachments.
- [ ] We can explain what would happen if a critical supplier became unavailable.

What to do next...

Any “no” is a useful starting point, not a failure. Prioritise suppliers that hold sensitive data, connect directly to your systems or support a service your business can’t operate without.

Supply chain security doesn't require a huge budget or a dedicated security team. It starts with understanding who and what your business relies on, creating clear expectations and regularly reviewing access, tools and supplier relationships. By taking a structured approach, you can significantly reduce your exposure to cyber threats while building greater resilience across your business.

The good news is that every improvement, no matter how small, makes a difference. If this guide has highlighted areas where you'd like additional support, Apex Computing can help you assess your current supplier landscape, identify risks and put practical controls in place that strengthen your security without slowing your business down.

Not sure where your biggest security risks are?

Book a complimentary cyber security review with our team today!

apex Computing Services

0161 299 0033

enquiries@apexcomputing.co.uk

www.apexcomputing.co.uk

Salford Quays, M50 3XW