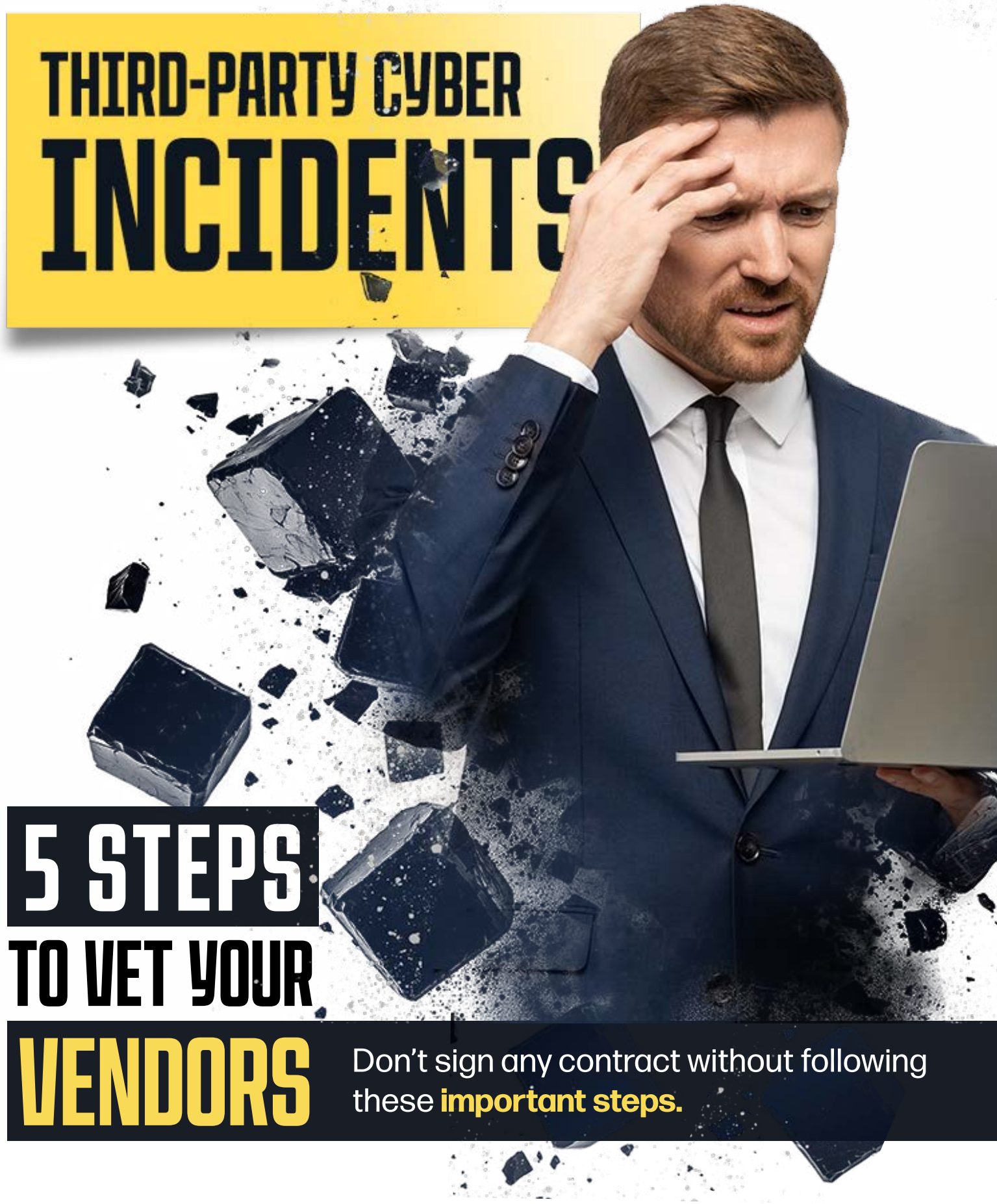
THIRD-PARTY CYBER INCIDENTS



5 STEPS TO VET YOUR VENDORS

Don't sign any contract without following these **important steps.**

Your third-party vendors are essential to your business,

but they can also introduce significant security risks.

Before signing a contract, vet the vendor's security practices by following these 5 steps:

1. Ask Vendors the **Right Questions**

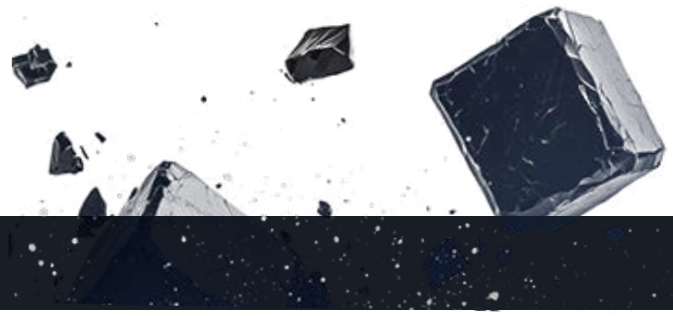
"What security protocols do you have in place?"

"What is your data breach recovery plan?"

"How do you respond to security incidents?"

2. Review **Security Audits** and **Certifications**

Ask for proof of certifications that the vendor has completed rigorous evaluations and adheres to industry-standard security practices.

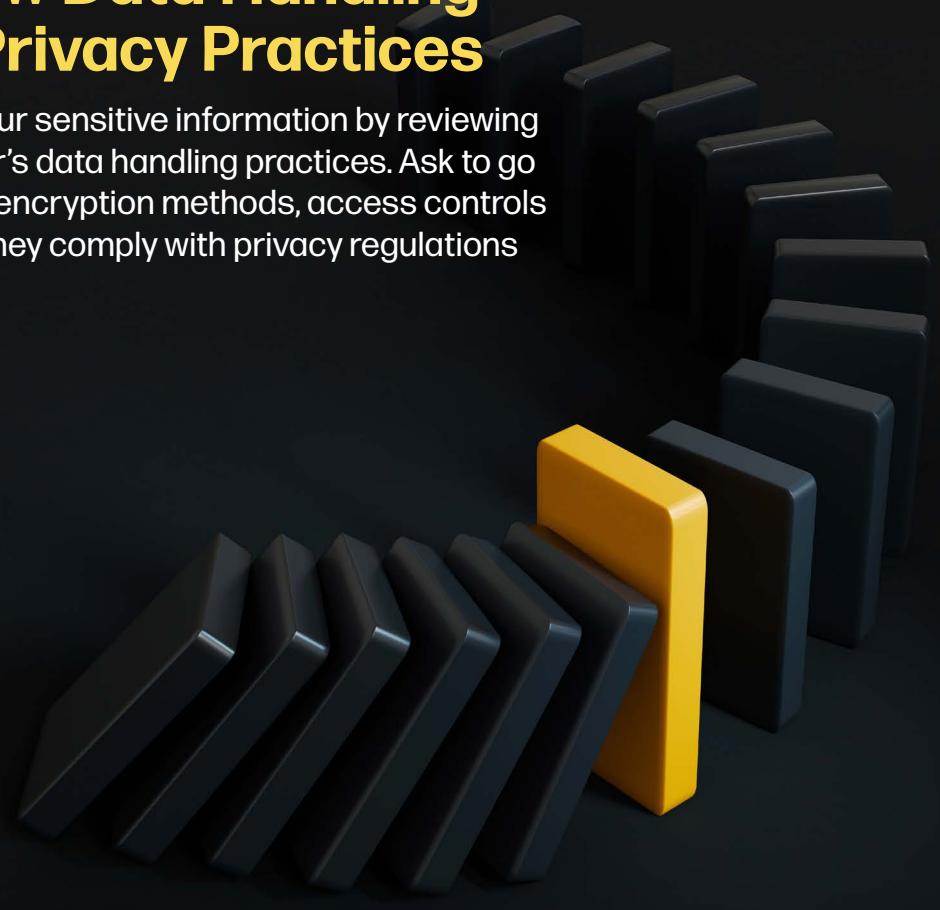


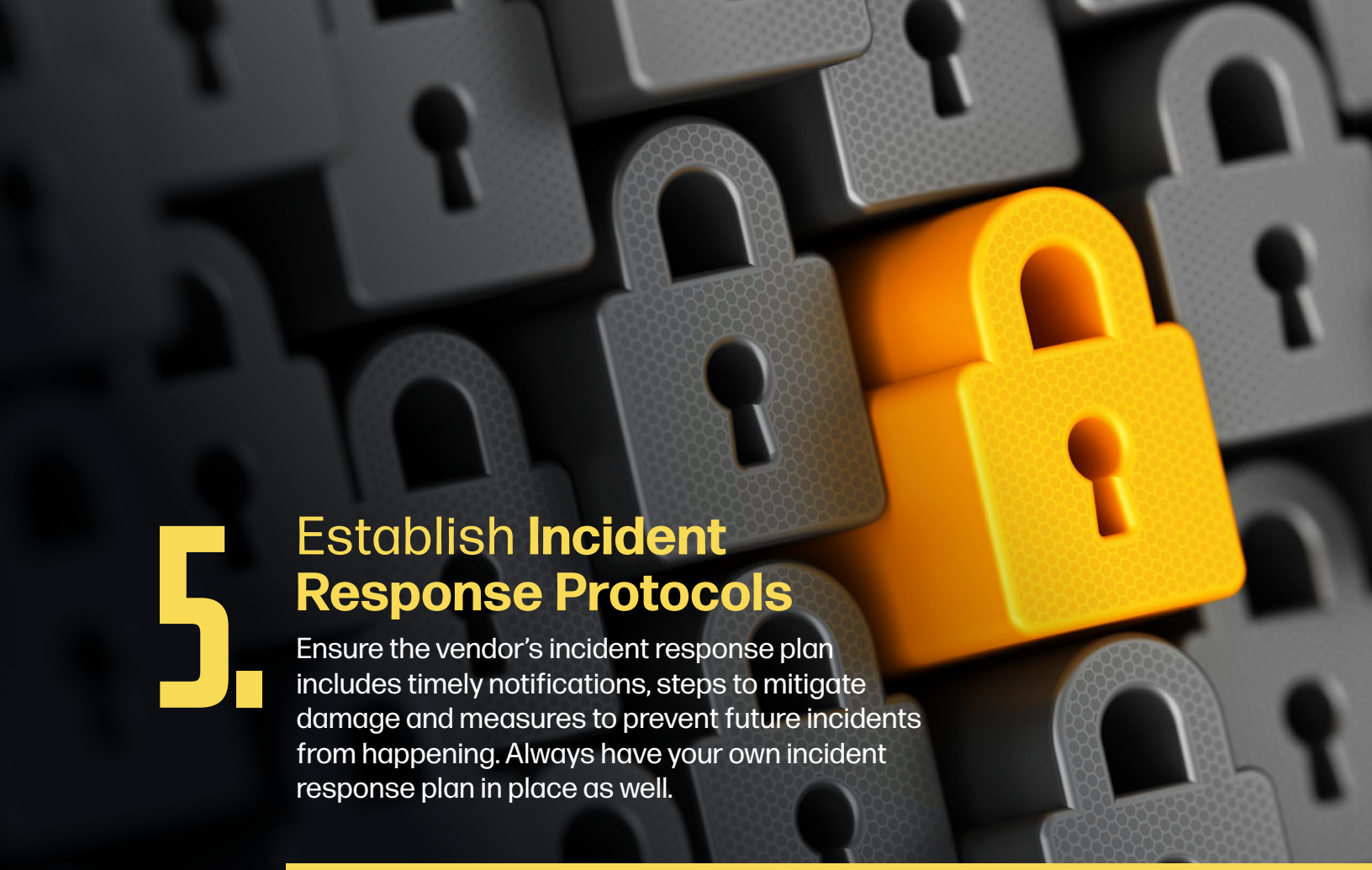
3. Assess **Financial Stability**

Financially unstable vendors may cut corners on security, leaving your business vulnerable. Vendors that have resources to maintain security best practices can better support your business in the long run.

4. Review **Data Handling** and **Privacy Practices**

Protect your sensitive information by reviewing the vendor's data handling practices. Ask to go over data encryption methods, access controls and how they comply with privacy regulations like GDPR.





5. Establish **Incident Response Protocols**

Ensure the vendor's incident response plan includes timely notifications, steps to mitigate damage and measures to prevent future incidents from happening. Always have your own incident response plan in place as well.

Not sure if your current vendors provide the safety measures needed to **protect your business**?

WE CAN HELP

Contact us for a **thorough third-party risk assessment.**