Third-Party Cyber Risk: Looking at Vendors' Cybersecurity

By: Jay Preall, Segal

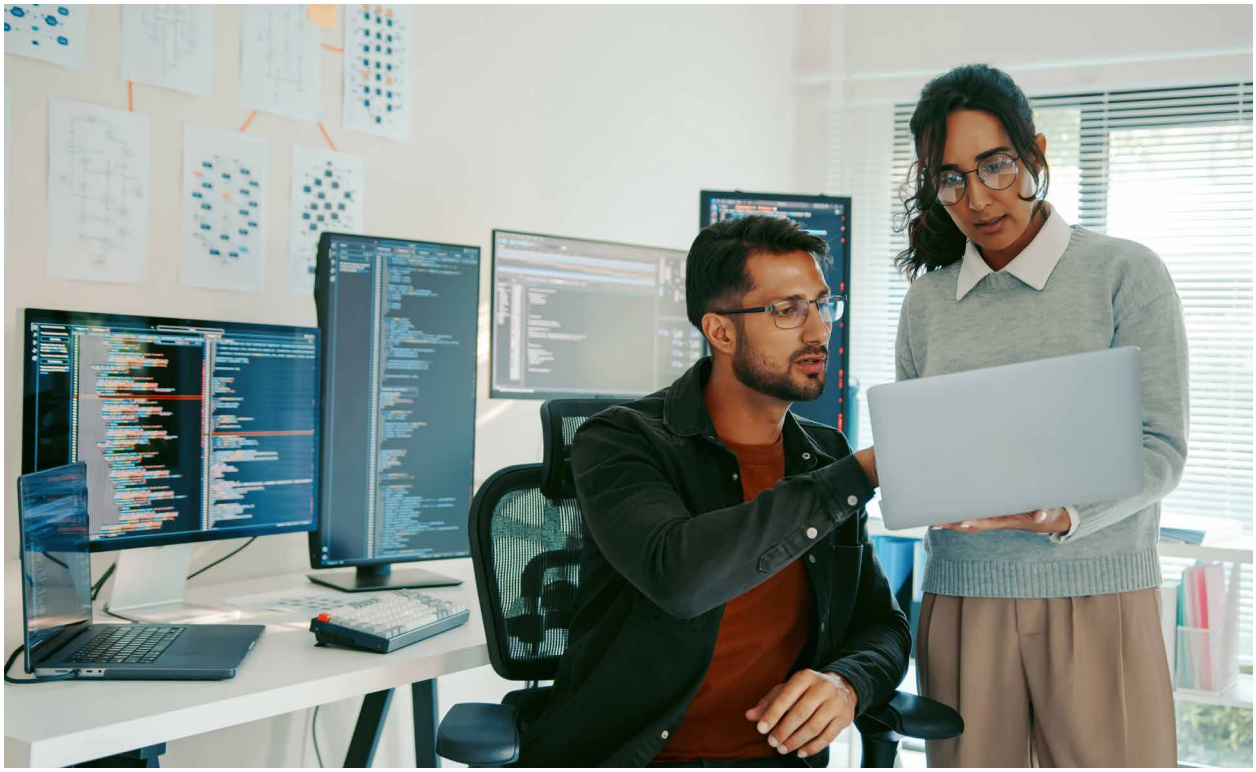

Photo Illustration © 2025, istock.com

Your vendors are a critical part of your success, especially if they provide services such as payroll, investing, or actuarial. Managing them is an important part of strong cybersecurity practices, because their helpful services could be putting you at risk. That's why regulatory bodies are now emphasizing the importance of third-party risk management and are expressing their concern during audits.

> *The more vendors you work with, the greater the chance you'll be impacted by a cybersecurity incident affecting one of them.*

Why it's critical to ensure your vendors aren't weak links

The Cyentia Institute and SecurityScorecard reviewed security measurements from more than 232,000 organizations and found that 98% of them have at least one third-party or fourth-party vendor that suffered a data breach in the last two years.[1]

The more vendors you work with, the greater the chance you'll be impacted by a cybersecurity incident affecting one of them. Compounding the risk is the fact that every vendor you work with likely works with other vendors, increasing the probability that you'll be affected by an incident.

Start with your vendor requirements

When choosing a vendor that will have access to any of your confidential data, start with your requirements. Potential vendors need to understand that cybersecurity is crucial and that any work they propose must come with assurances that your data is safe.

Potential vendors need to understand that cybersecurity is crucial and that any work they propose must come with assurances that your data is safe.

The vendor should provide a review of its cybersecurity protection program

If a vendor cannot provide an objective, third-party cybersecurity assessment, like a SOC2 report or other attestation, showing that it has solid cyber protections in place, that's a red flag.

An assessment should include:

- How often external, objective cybersecurity assessments are done
- How the people who will be handling your data are screened
- How the vendor monitors its own vendors from a cybersecurity perspective
- How the vendor tests its own applications to ensure they are secure
- What security governance policies are in place and being enforced, including protecting your data from becoming source material for artificial intelligence language learning models

Put it in writing

Vendors handling your confidential data should be willing to sign an agreement to clearly identify their roles and responsibilities if a cybersecurity incident occurs. This agreement should:

- Identify how the vendor will notify you of a cyber incident at their organization and how quickly that notification will occur.
- Require the vendor to maintain enough cyber liability insurance to cover potential breaches or losses of your data.
- Specify that the vendor is responsible for all of costs relating to a cybersecurity incident, including your costs, if the incident happened as a result of the vendor falling victim to a cyberattack.
- Dictate how much downtime you are willing to accept if the vendor has a cybersecurity incident.
- Confirm that the vendor is willing to participate in cybersecurity testing or simulations at a frequency you identify.
- Describe how your data will be handled during the contract and when the contract ends, including data retention requirements and returning or destroying your data upon contract termination.
- Ensure the vendor has similar agreements in place with all their vendors handling confidential data or having access to their systems.

If you need services from a vendor that does not have the size or financial wherewithal to implement full cybersecurity protection, the risk you are willing to accept from that vendor should be documented clearly in your contract to avoid unnecessary legal issues if an incident occurs.

By monitoring vendor performance, you can manage third-party cyber risk

Once you've contracted with a vendor, you should routinely monitor their performance to ensure they are meeting your contractual cybersecurity requirements. Consider these steps:

- Review daily, weekly, or monthly reports from the vendor's cybersecurity monitoring tools to show their protections are in place and working.
- Audit the vendor site and perform your own cybersecurity review and/or assessment.
- Ask the vendor to provide annual copies of approved and objective third-party cybersecurity assessments.
- Contract with your own cybersecurity experts to do penetration testing against your vendor (with your vendor's knowledge that the tests are occurring, of course).

Taking these steps will help you manage third-party cyber risk. See here for more on cybersecurity consulting. ◆

Jay Preall *is a Senior Consultant in Segal's Administration and Technology Consulting practice. Jay has more than 40 years of experience as a systems integrator. Jay works with pension and benefits systems clients on modernizing business processes and technology solutions.*

Endnotes:

[1] Cyentia Institute and SecurityScorecard, Close Encounters of the Third (and Fourth) Party Kind, February 1, 2023.