BURR FORMAN LLP

Cybersecurity Checklist for Vendor Management – Vendor Security

Article
02.15.2023

RELATED PROFESSIONALS

India E. Vincent, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

By now, you have heard many news stories about debilitating cyberattacks that started with the compromise of a vendor's systems and ultimately wreaked havoc on that vendor's customers. As a result, many businesses are seeking ways to ensure their vendors are utilizing proper security measures. Doing this requires drawing a fine line between validating the security of the vendor's operations while not extending control in such a way your organization could be seen as assuming responsibility for the vendor's IT systems. This article highlights some key items for vendors and customers to discuss when evaluating and establishing new relationships.

The Customer - Vendor Relationship

When selecting a vendor, consider data privacy and cybersecurity risks right from the start. How much data will the vendor need to access? Can that be limited in any way? Does the vendor require access to your computer systems – either on-site or remotely? Can the vendor's work be done without such access, or is there a way to monitor that access? The first consideration for both the vendor and the customer should be to determine if there are ways the amount of data exchanged or the extent of the access into the customer's computer systems can be limited. Limiting the access is almost always beneficial to both parties, limiting risk that results from the interaction as well as limiting any exposure if a breach occurs.

Cybersecurity Checklist for Vendor Management – Vendor Security

Once the risk is assessed and limited to the extent possible, the next step is to determine what security standards will apply. In most cases, the customer will be the data controller (party responsible for the data) and the vendor will be the data processor (handling the data on behalf of the customer). Because the data controller has responsibility to the individuals owning the information, laws typically require the data controller to ensure the data processor complies with all applicable security requirements. In the case of a vendor relationship, this means the customer has the responsibility to require the vendor to follow all data privacy laws and regulations and to properly secure its systems. Vendors should keep in mind that many customers are under legal obligations to impose these security standards, while customers should keep in mind that security standards do not have to be a one-size fits all, and different standards may apply to vendors with different risk profiles based on the services they are providing.

The Vendor's Security Posture

After determining the operational aspects of the customer - vendor relationship, the customer needs to evaluate the vendor's security position, including the technical, administrative and physical security measures in place and processes and procedures the vendor utilizes to protect data and its systems. This is the vendor's opportunity to demonstrate it meets all the requirements specified by the customer, and for the customer to demonstrate it has conducted proper due diligence before disclosing any data or allowing access to its systems.

When vetting the security posture of a potential vendor, customers should do enough to be comfortable the vendor meets both its legal requirements and the customers' internal security requirements, but not so much that they take on, or give the appearance of taking on, responsibility for the vendor's systems. Some organizations will choose to vet new vendors through completion of a security questionnaire, while others may require actual technical reviews or audits of the vendors' system. The approach each customer chooses should account for the organization's internal capabilities and capacity to conduct such audits and/or assess responses to a questionnaire.

Regardless of how the assessment is approached, these are just a few questions that should be addressed:

- Does the vendor have internal security policies and procedures such as an Information Security Policy, an Incident Response Plan, and a Business Continuity/Disaster Recovery Plan?
- Are those plans regularly reviewed and updated?
- Has the vendor properly documented its network environment in order to monitor operations of the network and track access to the system?
- What type of user authentication and access controls does the vendor utilize? Some examples of controls that might be discussed are multi-factor authentication, firewalls, intrusion detection and prevention services, end-point monitoring, and packet filters.
- What steps does the vendor take to ensure any risk posed by employees are minimized? Does it conduct background checks?

Cybersecurity Checklist for Vendor Management – Vendor Security

- Does the vendor require regular data privacy and security training for its personnel?
- Does the vendor segment data by customer so one customer's data is not mixed with data of other customers?
- Does the vendor utilize encryption for data in transit, in storage, and being disposed of?
- What type of security risk assessments, penetration testing, and vulnerability scans does the vendor conduct, and how frequently does it conduct these assessments?
- Does the vendor have a back-up system(s), business continuity plan, and disaster recovery plan? Are those systems and plans tested on a regular basis? Where are the back-ups stored, and how frequently are they updated?

Vendors with a sophisticated security position may have a prepared security statement in place to provide customers with most, if not all, of this information, but at other times the customer and vendor may need to work together to collect the information required to meet the customer's requirements. Customer organizations that do not have the resources to conduct an audit internally or to properly review and assess responses to vendor security questionnaires should consider engaging a consultant to assist with the process or provide training for internal personnel to develop the capability.

Once the operational aspects of the relationship have been assessed for inherent risk, and the vendor's security posture has been evaluated and deemed sufficient, it is time to work with your legal counsel to ensure the vendor agreement properly documents each party's obligations concerning security and data privacy.

If you could use some assistance determining what type of due diligence you should conduct for vendors, or if you are a vendor and would like assistance documenting your security safeguards for customers, feel free to contact a member of our Cybersecurity and Data Privacy team or other Burr & Forman attorney with whom you work.