Questions to ask your key suppliers about their IT security

As well as thinking about your organisations own cybersecurity processes, it is also important to think about your key suppliers, who may well have an impact on your own cyber risks. Your organisation's key suppliers often have access to sensitive and valuable information and data that you own, or their ability to function might directly impact your own ability to access your data that they might be hosting for you.

If suppliers do not protect this data adequately, they may be putting your organisation at risk of a cybersecurity or data protection breach. It is therefore an important part of your own cyber risk assessment, that you ensure that your suppliers follow data security best practices to improve cyber resilience.

IT security questions for your suppliers

1 What policies and procedures do you have in place for protecting your critical IT systems?

It is important that you understand how your supplier is storing, maintaining, securing and protecting data. What steps are they taking to mitigate the risk of breaches or downtime? Do they have appropriate standards and safeguards in place? Are they monitoring their cyber defences and do their physical systems meet recognised best practices? Who in the supplier's organisation is ultimately responsible for cybersecurity? Do they have the appropriate/required skills?

2 What security measures do you have in place to safeguard your systems?

It is important to understand what measures your supplier uses, there are many an organisation can put in place, including multi-factor authentication on all devices where data can be accessed (including personal devices), network security measures, up to date systems and software, physical security measures etc. Does your supplier utilise cybersecurity monitoring services?

3 How and when do you notify clients of security vulnerabilities or breaches?

It is the policy of some vendors not to disclose a security vulnerability unless it impacts a particular client's data. It is important to understand how and when they will notify you of any security issues and how they categorise risks and security issues.

4 Do you separate customer data from the main infrastructure?

For any data that is being housed with a supplier, you should have an understanding of the security controls in your supplier's environment and if your data is separate from their data, or that of their other clients, as this will reduce the risk of unauthorised access of your data.

ramsac
the secure choice

ramsac
the secure choice

5 Where are you storing my data geographically?

If there is a breach and your data is stored in another country, you may be subject to that countries data breach and privacy laws. Similarly, you may have restrictions in place by your own clients or professional bodies, which define where your data is stored, so you need to understand exactly where your suppliers are physically hosting your data. For example if your supplier offshores any data processing (in particular outside of the EU) they are then subject to the rules of data handling under GDPR.

6 Do you have data security/cyber liability insurance?

Most vendors have some form of professional liability insurance that will protect them during a data breach, but it may not protect your organisation, as it may not extend to third-party data or systems. Therefore, it is important to understand if your supplier's cyber liability insurance policy protects your data as well. If not, you may want to consider getting your own cyber liability insurance policy to cover any potential gaps.

7 How do you store and transfer data?

The best security in the world is worthless if it is being transferred in an unsecure manner. Make sure that the vendor has end-to-end encryption for file transfers. Also, consider requesting that your data be encrypted while being stored/at rest.

8 What recovery time is stated in your disaster recovery plan and when was this last tested?

Organisations should know how their vendor will restore their data and service in the event of a disaster, such as a ransomware attack. Does your supplier have a robust cyber incident response plan and general disaster recovery plan that is regularly tested, and improvements made where needed?

9 When was your last penetration test or external cyber audit?

Your supplier should carry out regular penetration testing and an external cyber audit, ask to see the results of these. Can the supplier provide a history of data or cyber breaches and what they have done to mitigate them?

Find out more

Checking supplier data security is an important part of your cyber resilience strategy. Speak to ramsac about how we can help you start building your cyber resilience strategy today.

Tel: **01483 412 040** email **info@ramsac.com**