THIRD PARTY RISK MANAGEMENT 101



Define an Incident Response Plan: Have a defined and tested incident response plan that includes procedures to follow in case of a security incident or data breach involving a third party.

Continuously Train Employees: Educate your staff about the importance of cybersecurity. Teach them to recognize potential threats from third parties. More importantly, train them on the procedures and processes to be followed when information must be shared with third parties.

Assess Vendors for Risk: Before partnering with a third party, assess their cybersecurity practices. This could be as simple as a questionnaire, or as complex as an on-site audit. Define a framework based on your organisation's context and risk appetite.

Embed Cybersecurity Clauses into Legal Agreements: Outline cybersecurity requirements in contracts and agreements. Work with legal experts and ensure incident notification requirements are outlined, as well as other steps to be taken in case of a breach.

Implemented Logging and Monitoring: Implement tools to log and monitor activities related to third-party access. This helps to detect and respond to unusual or suspicious behaviours related to third parties.

Enforce the Principle of Least Privilege: Limit access to sensitive information. Third parties should only be allowed access to resources and data that they absolutely require to perform their contracted services.

Encrypt Data before sharing it with Third Parties: Ensure that all sensitive or confidential data exchanged with third parties are encrypted. This provides an extra layer of protection against unauthorized access. Remember, in most cases once you have shared the information, you lose control over the information.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time