CPAs & ADVISORS

Cybersecurity Check-Up

GRF CYBERSECURITY SERVICES

Is your organization focused on the right issues when it comes to cybersecurity?
To help you identify and prioritize the most critical risks, GRF has developed comprehensive checklist you can use to help identify vulnerable areas.

- Have you identified your most critical assets and performed a risk assessment on them?
- Do you have a formally documented information security policy outlining organizational security objectives?
- Have you defined and identified sensitive data for the organization?
  - Do you know where this data is stored?
  - Is your sensitive data protected by least privilege access controls?
  - Are employees aware of how to send sensitive data? (e.g. Must be sent through secure channel or file sharing service)
- Do you have a documented password policy in place?
  - Does it require complex passwords, enforce password history, special characters, and length requirements?
  - Do you monitor for breached credentials?
- Do you have multifactor authentication enabled for applications, especially on admin accounts?
- Are updates applied to computer operating systems, anti-virus, anti-malware, firewalls, etc. on a regular basis?
- Do you have anti-virus installed on all devices touching your network?
- Do you review third parties on a regular basis to ensure they have adequate security measures in place and to verify that the service is still in use?
- Are employees completing regular security awareness trainings?
  - Is there a phishing simulation program set up?
- Do you have clear guidelines for submitting incidents for end users?
  - Is an incident response plan in place?
- Do you have a business continuity plan?
- Does it include all applicable third parties such as financial applications, web hosting, file storage, etc.?