COMPEER FINANCIAL®

QUESTIONS FOR YOUR IT PROVIDER

Even if you don't have a technical background, there are questions you can ask your current IT or security provider to determine if they are providing the ideal IT risk management you're looking for. Follow the guided questions below to begin a dialogue with your current provider or one you are vetting as a good fit.

1. **How do you make sure we update software, operating systems, applications and firmware on IT network assets in a timely manner?**
2. **Do we have software that is no longer supported by the vendor?**
3. **Do we enforce Multi-Factor Authentication (MFA) for all users, without exception?**
4. **Is MFA enforced on all VPN connections? If MFA is unavailable, can we require employees to use strong passwords?**
5. **How often do you review, validate or remove privileged/administrative accounts? Do they all have unique, individual passwords?**
6. **Have you configured and secured internet-facing network devices, disabled unused or unnecessary network ports and protocols, encrypted network traffic, and disabled unused network services and devices?**
7. **Do we have any of these exposed to the internet: Commonly exploited enterprise network services, including Link-Local Multicast Name Resolution (LLMNR) protocol, Remote Desktop Protocol (RDP), Common Internet File System (CIFS), Active Directory and OpenLDAP.**
8. **Is our network segmented to limit or block lateral movement by controlling access to applications, devices and databases?**
9. **How do you monitor the attack surface and investigate abnormal activity that may indicate lateral movement of a threat actor or malware?**
10. **What security tools, such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tools, do we have?**
11. **How can we monitor the environment for potentially unwanted programs or implement application control?**
12. **Do you back up our critical systems and, if so, do you ever test them?**
13. **What is our incident response plan if we suffer a breach or ransomware attack?**
14. **Can you provide security awareness training to our employees?**