



Questions You Need to Ask Your IT Department About Your Company's Security

Internal Security:

- How often are we changing employee passwords? What complexity requirements do we have for our passwords?
- How are we addressing the potential risk imposed by our employees as users? How much control do our users currently have over their computers?
- Are we training employees on security awareness and educating them on internet and device use policies?
- How are we protected from BYOD devices in the workplace?
- What preventative measures are we taking to protect against the actions of disgruntled employees?

Cybersecurity:

- Where is our business most vulnerable to cybercrime?
- What are we doing to address our most significant cyber threats?
- Have we allocated enough resources to cyber security and are we staying current?
- How are we able to identify and remediate cyber threats? Are we using multiple security technologies to achieve this?
- What firewall are we using and does it utilize the most current threat detection and prevention methods?
- What resources are you using to stay current on the security landscape?

Backup and Recovery:

- How long can our company afford to be down in an emergency?
- Is our sensitive data secure both in transit and in storage?
- What data loss prevention policies (DLP) do we have in place? Do they address USB access?
- Where are we storing our data and how is it protected?
- How frequently are we backing up our data?
- Do we test the recovery of our backups on a regular basis?
- What is our documented disaster recovery plan and when was it created, reviewed or updated?
- Who has been trained on our DR plan?

Business Considerations:

- Are there any third-party applications on our network that could put our security at risk? What safeguards do we have in place?
- How are we ensuring that we are meeting regulatory compliance for our industry and how are we staying current with changes?
- Is unsanctioned device or application use a threat to our business? How is that being addressed?
- What is being done to protect our wifi network? Are our internal and guest wifi separate?
- What do we need to be doing now to continue to protect our company moving forward?