IT Environment Security Checklist

It's important for all organizations to review and update their security systems. To help you maximize protection in your IT environment, this checklist that can serve as a starting point to improve your security posture.

Cybersecurity Threat Mitigation

A goal for every organization that is looking to mitigate cyber-attacks is to collectively work towards better security. You can do that by implementing the following measures:

- [ ] Document your security policies
- [ ] Enforce security policies with training and controls
- [ ] Ensure compliance with appropriate compliance frameworks with internal and external audits
- [ ] Have a dedicated individual/team for security-related tasks

Employee Security

Your employees are your first line of defense against cyberthreats. You can strengthen your security framework by taking the necessary steps to monitor and safeguard them. Following are some security measures to take:

- [ ] Implement Multi-factor Authentication (MFA) to protect sensitive data
- [ ] Enforce strong password policies
  - [ ] Use a password management tool to avoid writing down passwords on post-it notes
  - [ ] Prevent reuse of passwords across multiple sites
  - [ ] Define policies to change passwords periodically for critical documents Include security awareness
- [ ] Include security awareness training at the time of onboarding
- [ ] Conduct periodic security tests to identify vulnerable employees who may fall victim to social engineering
- [ ] Have an email phishing protection in place
- [ ] Enable Single Sign-On (SSO)

Password Security

Since most cyberthreats originate from stolen credentials, you need to educate your employees about password security.

- [ ] Enforce host-proof hosting of sensitive passwords
- [ ] Control security access of passwords
- [ ] Create policies against simple passwords
- [ ] Use different passwords for all your main accounts
- [ ] Avoid entering passwords on computers you don't control

Endpoint and Network Security

Outdated endpoints and poor security hygiene are a deadly combination that attracts various threat actors. You can ensure maximum endpoint and network security through the following measures.

- [ ] Set up recurring tasks to keep remote management software up to date
- [ ] Use third-party patching to patch all the endpoints regularly
- [ ] Set up automated notifications for malicious or suspicious activities
- [ ] Restrict access to remote management tools
- [ ] Have a dedicated individual/team to periodically check and manage the network's settings and software upgrades
- [ ] Place firewalls between endpoints within a network to restrict host to host communication

Backup

Backup is an absolute requirement for companies of all sizes. Choosing the right backup can save you a lot of time and help you resume operations instantly following a security incident. Make sure you incorporate the following measures in your backup.

- [ ] Ensure your data is being backed-up regularly
- [ ] Use the 3-2-1 strategy to backup multiple copies in different storage media
- [ ] Have a backup in place for your entire system (including hardware, software, servers, external files, tools, etc.)
- [ ] Regularly review and update your backup policies
- [ ] Test your backups regularly
- [ ] Have a disaster recovery plan that minimizes downtime following an incident