Checklist for Better Security

ADAMS BROWN
Technology Specialists
above+beyond

By following these steps and regularly reviewing and updating cybersecurity measures, you can significantly reduce the risk of a successful cyberattack and minimize the potential damage if one does occur.

TECHNOLOGY

- [ ] Keep all software and systems up-to-date with the latest security patches
- [ ] Implement multi-factor authentication for all accounts
- [ ] Use firewalls and antivirus software to protect against cyberattacks
- [ ] Implement email filters to prevent spam and phishing emails from reaching employees
- [ ] Use encryption for sensitive data, both in transit and at rest
- [ ] Use virtual private networks (VPNs) to access company networks and systems remotely
- [ ] Use intrusion detection and prevention systems to monitor network traffic for potential attacks
- [ ] Use role-based access control to ensure employees only have access to the data and systems they need to perform their job duties
- [ ] Use secure file transfer protocols (SFTP) to transfer sensitive data
- [ ] Use secure cloud storage providers to ensure data is encrypted in transit and at rest

PEOPLE

- [ ] Address the cybersecurity talent gap and build the resources you need to stay safe
- [ ] Use strong, unique passwords for all accounts and encourage employees to do the same
- [ ] Educate employees about cybersecurity best practices, including identifying and reporting suspicious activity
- [ ] Conduct background checks on all new hires to reduce the risk of insider threats
- [ ] Conduct regular security awareness training for employees

PROCESSES

- [ ] Address compliance regulations
- [ ] Limit access to sensitive data and ensure access is granted on a need-to-know basis
- [ ] Back up data regularly and store it securely
- [ ] Monitor systems for unusual activity and investigate any suspicious activity immediately
- [ ] Conduct regular cybersecurity assessments to identify potential vulnerabilities and proactively address them
- [ ] Develop an incident response plan to ensure all employees know what to do in the event of a cyberattack
- [ ] Develop and regularly test a disaster recovery plan to ensure critical systems and data can be quickly restored in the event of a disaster
- [ ] Use secure file transfer protocols (SFTP) to transfer sensitive data
- [ ] Use secure cloud storage providers to ensure data is encrypted in transit and at rest

Remember that despite taking all necessary precautions, a breach can still occur. You still need to have a response plan.