

Information Security Checklist

This checklist is for educational purposes only and does not create an attorney client relationship. The BPE Law Group recommends businesses consult their Information Technology professional for actions specific to their situation.

- **Implement a multi-layered defense**
 - Intrusion Prevention System (IPS). Think of an IPS as the guard in front of the castle gate. An IPS examines network traffic and blocks suspicious behavior.
 - Firewall. A firewall is like the castle gate, preventing bad actors from getting into the castle. A firewall prevents unauthorized access using a set of rules.
 - Intrusion Detection System (IDS). An IDS is like a security patrol inside the castle. An IDS monitors your internal network and blocks harmful activities.
 - Endpoint Security. Think of this as people inside the castle locking the door to their home. End user devices – servers, laptops, desktops etc – need their own individual security software to “lock the door” and maintain security.
- **Help your people stay secure**
 - Have written policies, so people know what is expected.
 - Provide periodic training to help your team members to spot risks and know what to do if a bad actor tries to get their password or other key information.
- **Make it harder for the bad actors.** Implement multi-factor authentication.
- **Keep backups.** Backups help if data is deleted, either accidentally or maliciously.
- **Cyber insurance.** Losing your client’s data could be very costly. Get insurance.
- **Stay compliant with the rules.**
 - There are a variety of security standards to help reduce risk. A few examples: Payment Card Industry Standards (PCI) for companies that take payment cards; HIPAA for companies that store protected health information.
 - Ask how your cloud vendors will protect your data.
 - Make sure your cloud vendors comply with rules you need to comply with.
- **Don’t Get Complacent.**
 - Good security requires vigilance and maintenance
 - Do you have procedures to keep your operating systems, applications, and anti-virus up to date?
 - Conduct periodic audits to ensure security controls are operating correctly.
 - Conduct periodic training to ensure your team members are security-aware.