Reducing a Small Business' Potential Cybersecurity Risks Checklist

1. Do a risk assessment of the company's information security practices.

- ☐ **Consider** unique aspects of the firm's business that may make it **vulnerable** to a certain type of attack (e.g. what type of information does the company handle?).
- ☐ **Carry out an audit** of any company data assets and consider a full data mapping exercise.
- ☐ **Assess** the business' use of mobile and personal IT devices, the strength of passwords, and the level of encryption for sensitive data.
- ☐ **Draft** a clear outward-facing **data security policy** and document in detail all internal procedures.

2. Implement new/additional security controls to reduce potential risks.

- ☐ **Malware protection**: make sure to install up to date anti-virus software.
- ☐ **Computer network**: should include firewalls, proxies, and access controls.
- ☐ **User privileges**: should be allocated based on need with controls in place to prevent unauthorized access.
- ☐ Install **user verification methods**, including use of digital signatures**,** and restrict use for removable media such as USB drives.

3. Assess the company's cloud computing practices.

- ☐ **Inventory** the firm's cloud-based platforms.
- ☐ **Analyze** whether it is appropriate to be sending that information to the cloud (i.e. is the information of a sensitive nature?).
- ☐ **Review** the business' **vendor management agreements** and seek to understand how third-party vendors are safeguarding data during transfers and while stored.
- ☐ Remind clients to check the addresses of any **emails** purportedly sent by the firm, especially if they relate to any financial information or requests for payment.

4. Take steps to make cybersecurity a part of the company's regular risk-management procedures.

- ☐ **Review systems and procedures** regularly and incorporate tests to improve security.
- ☐ **Dispose** of programs or physical devices that are no longer needed.
- ☐ **Consider cyber insurance coverage**

5. If the company experiences a cyber attack

- ☐ **Remove** any immediate and ongoing threats
- ☐ **Conduct** a post-breach review
  Comply with breach notification laws