SBDC
PENNSYLVANIA

Small Business Development Centers
Helping businesses start, grow, and prosper.

Opening

1. **Are you using an outsourced Technology firm to manage your security, servers, anti-virus, malware, etc.**
   - **Yes or No**

2. **How are you managing the infrastructure decisions with your hardware and software, e-commerce, website activity, etc.**
   - **Using an IT firm and receiving frequent reports for review**
   - **Google Analytics and/or reactive to problems as they occur**
   - **Need to develop a technology/security plan**

A. Risks – Assessing Vulnerabilities

3. **Do you manage your own server/s?**
   - **Yes or No**

4. **Have you identified the confidential data/reports (credit card numbers, social security numbers, etc.) collected or stored on your servers/computers?**
   - **Yes or No**

5. **Do your employees receive on-going training to identify phishing emails?**
   - **Yes**
   - **Partial, our employees have limited knowledge and training**
   - **No**

6. **How do you restrict employee access to confidential information stored on your servers/computers?**
   - **Only senior level management has access to confidential information**
   - **Only individuals with prior approval have access to confidential information**
   - **All employees have access to confidential information**

7. **How often does your business update the operating system on devices that have access to confidential information?**
   - **Automatically**
   - **Manually on a regular basis**
   - **Manually, but only if the application is supported by the developer and compatible with our version**
   - **Irregular, infrequent, or not being monitored**
   - **Not sure**

8. **Have you identified all of the devices that store or have access to confidential information?**
   - **Yes or No**

9. **Do you remove non-essential applications from business hardware?**
   - **Yes or No or Not sure**

B. <u>Protect – What basic practices do you have to protect your systems?</u>

10. **How do you manage your employee's passwords?**
    - **All users have their own logins**
    - **Some systems use a common login**
    - **No logins in place/one shared login**

11. **How complex are your passwords?**
    - **At least 8 characters containing upper-case and lower-case letters, numbers, symbols**
    - **Undefined number of characters, but requires upper-case or lower-case letters, or numbers or symbols**
    - **No specific guidelines are required**

12. **How often do you change your passwords?**
    - **More than once a year**
    - **Once a year**
    - **Never**

13. **Do your computers automatically time-out after a duration of inactivity?**
    - **Yes or No**

14. **How does your company utilize firewalls in order to block unauthorized access?**
    - **We have a separate firewall built within our company to protect our internal network**
    - **We use the internal firewall installed on our Windows or Apple computers**
    - **We do not use firewalls**
    - **Not sure**

15. **How often do you train your employees on the company's cyber security policy and procedures?**
    - **They are trained on hire and annually**
    - **They are trained monthly**
    - **They are trained as-needed**
    - **They are never trained**

16. **Do you allow your employees to access company files remotely?**
    - **We do not allow remote access**
    - **Employees use a VPN to connect securely**
    - **Employees do not access sensitive information over public WIFI connections**

C. **<u>Detect – Prevention and reaction to threats</u>**

17. **Does your business have anti-virus software?**
    - **Yes, on all our devices (desktops, laptops, tablets, phones etc.)**
    - **Yes, but only on some devices**
    - **No, our devices do not have antivirus software**
    - **Not sure**

18. **Does your business have anti-malware protection?**
    - **Yes, on all our devices (desktops, laptops, tablets, phones etc.)**
    - **Yes, but only on some devices**
    - **No, our devices do not have malware protection**
    - **Not sure**

19. **Is your business up to date in order to detect viruses or malware?**
    - **Yes, our business is up to date.**
    - **No, we are not up to date**
    - **Not sure**

20. **How often do you check your devices for any malware attacks?**
    - **Weekly**
    - **Monthly**
    - **Annually**
    - **Never**

21. **Did you know that liability insurance does not cover a breach?**
    - **Yes or No**

D. **<u>Respond – Be offensive and defensive with a breach if or when it occurs</u>**

22. **How often do you backup your data?**
    - **Daily**
    - **Weekly**
    - **Monthly**
    - **Never/Don't know**

23. **In the event of a cyber-attack, what response plan do you have in place? (Check all that apply)**
    - **Immediately back-up sensitive data**
    - **Contact Response Team**
    - **Preserve files for further investigation**
    - **None of these apply**

24. **Have you ever had a security breach?**
    - **Yes or No**

25. **If no, what would you do in the event of a security breach? (Check all that apply)**
    - **Immediately back-up sensitive data**
    - **Contact Response Team**
    - **Preserve files for further investigation**
    - **None of these apply**

26. **A good practice for when a cyber-attack does occur is to have an individual or group of individuals assigned to not only control the attack, but to discover how or where the attack occurred. Do you have an individual or group assigned to do that?**
    - **Yes, they are readily accessible and well-training in this area.**
    - **No, we would like to but to not have an individual or group capable of carrying out these tasks at this time.**
    - **No, we would establish this practice after an attack occurred.**

E. <u>Recover: How will you get your business back to normal after a breach?</u>

27. **Do you purchase cybersecurity insurance?**
    - **Yes or No**

28. **Do you have easy access to contact information for the following resources that can help you recover? (Check all that apply)**
    - **A legal agency which specializes in cyber crime**
    - **Internet service provider**
    - **List of software/hardware vendors who supplied your systems/devices**
    - **None of these apply**

29. **Do you have a detailed recovery plan that says what actions you and your employees will take to bring your business back to normal following a cyber-attack?**
    - **We have a recovery plan in place that lists clear, comprehensive steps**
    - **We have part of a recovery plan, but it may be short or vague**
    - **We do not have a recovery plan in place**

30. **Did you know that businesses must meet a minimum security standard in order to get a payout from cybersecurity insurance?**
    - **Yes or No**

31. **Is there someone in your organization who is designated to manage recovery after a cyber-attack?**
    - **Yes**
    - **No, but our employees have been trained on the proper way to respond**
    - **No**

32. **PA law requires that your business notify customers if their confidential information has been or might have been stolen. Does your business have a plan in place to notify customers if that occurs?**
    - **Yes, we can quickly notify our customers.**
    - **Yes, but we would have to figure out how to notify our customers.**
    - **No, our business does not keep any permanent records of customer information and could not notify them**

33. **Have you ever attempted to restore your backed up data to make sure it is functional?**
    - **Yes or No**