CyberFirst Solutions LLC

Securing your business first

Cybersecurity Questionnaire

Business Questions

1. Is cyber security a priority for your business?

- (0) Not sure
- (1) No
- (2) Yes

2. Has someone in your business been given responsibility for cyber security?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is this an ongoing role, supported by management (circle if yes)?

3. Has your business completed a cyber security threat and risk analysis (of any kind)?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, are risks prioritized and tracked with regard to reducing them (circle if yes)?

4. Does your business have a Cyber Security Plan?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is it being followed (circle if yes)?

5. Does your business have a Cyber Security Policy?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is it supported through security awareness training for employees (circle if yes)?

6. Does your business have a Disaster Recovery Plan?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is it kept up to date and has it been tested (circle if yes)?

7. Does your organization provide employees with guidance on the handling and labelling of sensitive information?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is this supported by policy or a standard (circle if yes)?

8. Does your organization provide employees with guidance on the secure use of mobile devices?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is this supported by a guideline and any mobile device management tools (circle if yes)?

Technical Questions

9. Is there a firewall installed between your business computers, including point-of-sale (POS) systems, and the Internet?

- (0) Not sure
- (1) No

- (2) Yes
- (3) If yes, is it regularly maintained and checked by someone with the appropriate training and experience (circle if yes)?

10. Does your business use an encryption tool (usually software) to secure sensitive information before sharing it outside of the business environment (such as with the transmission of email attachments)?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, do all personnel know how to use the tool and is usage monitored and enforced (circle if yes)?

11. Does your business have a spam filtering or blocking solution in place?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, do all personnel know how to report spam that is threatening or seems to be part of an attempt to solicit personal or sensitive business information (circle if yes)?

12. Does your business use an anti-malware solution?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, is it installed on all of the business's computers and is it regularly (usually hourly or daily) updated (circle if yes)?

13. Does your business follow best practices for strong passwords and password protection?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, are strong password rules enforced (circle if yes)?

14. Does your business back up data and applications on a regular basis (usually daily or more frequently)?

- (0) Not sure
- (1) No
- (2) Yes
- (3) If yes, are backups tested on a regular basis and are some backups kept off site in case of disaster (circle if yes)?

15. Does your organization provide personnel with guidance on working in a secure manner when travelling or otherwise outside of the business environment?

- (0) Not sure
- (1) No
- (2)Yes
- (3) If yes, is this supported by use of a virtual private network (VPN) (circle if yes)?

You have finished the self-assessment questionnaire.

If your score was **0-to-15** then you should consider reading this whole guide, as soon as you can. Then, consult with others in the business to begin planning and implementing cyber security in your business.

If your score was **16-to-30** then it's safe to say that your business has done some work with respect to cyber security. However, you likely need to do more and should read the guide with particular focus on those areas where you scored low.

If your score was **31-to-45** then your business has made good progress in several areas of Cyber security. However, new threats are constantly developing and it will be important to still consider the topics in this guide and discuss next steps (as appropriate).

12.2 Appendix B: Glossary

Assets: Any items belonging to or held by the business, with some value (including information, in all forms and computer systems).

Attack: An attempt to gain unauthorized access to business or personal information, computer systems or networks for (normally) criminal purposes. A successful attack may result in a security *breach* or it may be generically classified as an "incident."

Authentication: A security practice implemented (usually through software controls) to confirm the identity of an individual before granting them access to business services, computers or information.

Backup: The process of copying files to a secondary storage solution, so that those copies will be available if needed for a later restoration (e.g., following a computer crash).

Breach: A security breach is a gap in security that arises through negligence or deliberate attack. It may be counter to policy or the law, and it is often exploited to foster further harmful or criminal action.

Cyber: Relating to computers, software, communications systems and services used to access and interact with the Internet.

Encryption: Converting information into a code that can only be read by authorized persons who have been provided with the necessary (and usually unique) "key" and special software so that they can reverse the process (e.g., decryption) and use the information.

Firewall: A firewall is a type of security barrier placed between network environments. It may be a dedicated device or a composite of several components and techniques. Only authorized traffic, as defined by the local security policy, is allowed to pass.

HTTPS: Hypertext Transfer Protocol Secure.

Identity Theft: Copying another person's personally identifying information (such as their name and Social Insurance Number) and then impersonating that person to perpetrate fraud or other criminal activity.

Malware: Malicious software created and distributed to cause harm. The most common instance of malware is a "virus."

Patch: An update to or repair for any form of software that is applied without replacing the entire original program. Many patches are provided by software developers to address identified security vulnerabilities.

Appendices

OS: Operating System.

OTP: One-Time Password.

Password: A secret word or combination of characters that is used for authentication of the person that holds it.

Phishing: A specific kind of spam targeting one or more specific people while pretending to be a legitimate message, with the intent of defrauding the recipient(s).

POS: Point of Sale.

Risk: Exposure to a negative outcome if a *threat* is realized.

Safeguard: A security process, physical mechanism or technical tool intended to counter specific threats. Sometimes also referred to as a control.

Server: A computer on a network that acts as a shared resource for other network-attached processors (storing and "serving" data and applications).

SMB: Small and Medium Business.

Spam: Email that has been sent without the permission or request of you or the employee it has been sent to.

Threat: Any potential event or action (deliberate or accidental) that represents a danger to the security of the business.

URL: Uniform Resource Locator.

Vulnerability: A weakness in software, hardware, physical security or human practices that can be exploited to further a security attack.

VPN: Virtual Private Network.

Wi-Fi: A local area network (LAN) that uses radio signals to transmit and receive data over distances of a few hundred feet.