**Appendix**

**Appendix I: Cyber Threat Definitions**

1. **Supply Chain Attack:** a cyber-attack that poses a risk not only to your company, but also to your suppliers and customers with whom you share communications via the internet.
2. **Spear / Whale / Phishing Emails:** fraudulent emails or social engineering techniques that appear legitimate with the aim to steal sensitive information such as payment details or login ID & passwords, or to install malicious software inside your computers.
3. **Ransomware:** Often spread through phishing emails, attachments, links or USB sticks that contain malware that employs encryption to hold your valuable systems ransom whereby you cannot operate unless you pay a ransom to the hacker in the hope they will decrypt and give you back access to your own files.
4. **URL interpretation/Broken Access Control:** A hacker could manually edit your company URL text in the web browser address bar to access private web pages to gain administrator privilege
5. **Man-in-the-Middle Attack:** An attacker positions himself in the middle of you and the server communicating directly with both parties who believe they are directly communicating with each other. The entire conversation is controlled by the attacker. This can be done anywhere with an unencrypted Wi-Fi access point on any devices that connect to it.
6. **Zero-Day Exploit:** Hackers hunt for and exploit your vulnerabilities, or faults in software that’s running on targeted machines which you would know nothing about, only the hacker who intends to cause maximum damage in the least amount of time.
7. **Denial-of-Service:** An attack intended to shut down a machine, server, service or network, by flooding the target with traffic or sending it information that triggers a crash.
8. **Injection:** Hackers could take advantage of your offsite website containing all your orders, personal customer information and payment details, by finding vulnerabilities in the database e.g. search boxes to inject malicious SQL statements to force the server to reveal information it normally wouldn’t.
9. **Trojan Horse:** A malicious program that is hidden inside what looks to be legitimate software, but once activated, enables hackers to gain backdoor access to your system where they can spy on you or steal your sensitive data without your consent.
10. **Drive by attacks:** Malicious programs that install to your devices without your consent and expose you to cyber-attacks. This could occur simply by a user visiting a legitimate, but compromised website. You wouldn’t have to click or download anything to enable the attack.
11. **DNS Spoofing:** Hackers redirect web traffic toward fake web servers and phishing websites. The hacker could deliberately construct a poor-quality website to harm your company’s reputation.
12. **Business email compromise:** The hacker could gain access to your business email account and impersonate your identity to defraud, you, your employees or customers
13. **Identification/Authentication Failures:** Hackers have various techniques to easily discover weak passwords, especially if your system only has single factor authentication.
14. **Cryptographic Failures:** Your sensitive data which falls under privacy laws e.g. passwords, credit card numbers, personal details if not stored securely, could easily accessed by hackers.
15. **Insecure Design:** If a well-built house rests upon weak foundations, then it is also weak. The same can be said for your systems if they are not designed with security in mind.
16. **Security Misconfiguration:** Inaccurate, insecurely configured security controls e.g. default settings.
17. **Vulnerable/Outdated Components:** If the software is unsupported, out of date, or obtained through unsecure links.
18. **Security Logging and Monitoring Failures:** Logins, failed logins and high value transactions that aren’t logged. Lack of or unclear warning/ error messages. Failure to monitor and log suspicious activity.
19. **Brute Force Attack:** Attacker submits every possible password combination until entering the correct one.
20. **Dictionary Attack:** A form of brute force attack where the attack submits every word in the dictionary as a password attempt.
21. **Rainbow Table Attack:** A huge database of precomputed hashes that attempts to discover the password from the hash.

**Appendix II: 3-2-1 rule for backing up data**

* Have 3 backup copies
* Have backups stored on two different types of media e.g. the cloud, hard disk, removable devices such as USB.
* Have one copy stored offsite in a different network.