RISK LESSON

Nancy Stevens – First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by
the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

RISK

DEFENSE IN DEPTH ACTIVITY

The following list of 25 cybersecurity controls are used to eliminate or reduce a) the likelihood that a threat source can exploit a vulnerability, and b) the impact if the threat source does exploit the vulnerability. You might need to read more about them online. Once you have familiarized yourself with them, you will complete the worksheet.

STEP 1

Select one of the four cybersecurity risk scenarios presented earlier, i.e., 1) Malware, 2) Identity Theft, 3) Ransomware, or 4) Business Email Compromise. Identify 5 controls from the list below that could be used in a layered or "defense in depth" strategy.

1. Anti-virus software
2. Anti-malware software
3. Multifactor Authentication
4. File Back Ups or cloud storage
5. Password Manager app
6. Credit Freeze
7. Encryption
8. File Integrity Monitoring
9. Firewall
10. Identification
11. Authentication
12. Identity Theft Protection or Insurance
13. Intrusion Detection/Alerts
14. Password Policies (E.g., password strength and rotation)
15. Redundancy
16. Risk Assessment
17. Software Patching/Patch Management system
18. Spam Filter
19. App permissions

20. Anti-phishing training program
21. System Logging
22. VPN software
23. Physical security
24. Screen locking of device
25. WiFi security

STEP 2

Define each of the 5 selected security measures, identify whether it is a preventive, detective, or corrective measure, and justify your selection of control measures. Fill in the table accordingly.

Preventive measures are meant to deter. Detective measures identify so that corrective measures can be implemented. Corrective measures help mitigate damage. (Complete the table below).

COMPLETE THE TABLE

Security Measure Provide definition	Type of Measure (Circle one)	Justification
	Preventive Detective Corrective	
	Preventive Detective Corrective	
	Preventive Detective Corrective	
	Preventive Detective Corrective	
	Preventive Detective Corrective	