Mapping the Critical Security Controls (CSC) v4.0 to the Verizon VERIS 2013 Threats - Executive Summary

VERIS 2013 Report Threats	Gap Analysis	Matching Controls	Match to Top Seven Human Risks (HR)
Controls that would help mitigate each of the VERIS threats.		CSC 1.1-10, 9.1-6	
1. Tampering (alter physical form or function)	* Threat is partially addressed.	CSC 1.6, 3.13	
2. Backdoor (enable remote access)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
3. Use of stolen authentication credentials	Threat is completely addressed.	CSC 14.1-11, 15.1-5	HR-1/HR-4
4. Export data to another site or system	Threat is completely addressed.	CSC 10.1-7, 13.1-14, 17.1-8	
5. Use of Backdoor or C2 channel	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
6. Phishing (or any type of *ishing)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	HR-1 / HR-3
7. Command and control (C2)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14, 13.1-14	
8. Downloader (pull updates or other malware)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
9. Brute force or password guessing attacks	Threat is completely addressed.	CSC 14.1-11, 15.1-5	HR-4
10. Spyware, keylogger or form-grabber (capture user input or activity)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
11. Capture data stored on system disk	Threat is completely addressed.	CSC 14.1-11, 15.1-5, 17.1-8	
12. System or network utilities (e.g., PsTools, Netcat)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
13. Abuse of system access privileges	Threat is completely addressed.	CSC 12.1-14, 14.1-11, 15.1-5, 16.1-12	*Note 1*
14. Ram scraper or memory parser (capture data from volatile memory)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
15. Use of unapproved hardware or devices	Threat is completely addressed.	CSC 1.1-12, 17.1-8	*Note 1*
16. SQL injection	Threat is completely addressed.	CSC 6.1-9	*Note 2*
17. Embezzlement, skimming, and related fraud	* Threat is partially addressed.	CSC 14.1-11, 15.1-5	*Note 1*
18. Theft (taking assets without permission)	* Threat is partially addressed.	CSC 1.1-10, 14.1-11, 17.1, 17.5	*Note 1*
19. Bribery or solicitation	* Threat is partially addressed.	CSC 12.1-14, 14.1-11, 15.1-5	HR-3/HR-6
20. Disable or interfere with security controls	Threat is completely addressed.	CSC 3.1-13, 10.1-7	*Note 1*
21. Password dumper (extract credential hashes)	Threat is completely addressed.	CSC 2.1-10, 3.1-13, 4.1-12, 5.1-17, 12.1-14	
22. Misconfiguration	Threat is completely addressed.	CSC 3.1-13, 10.1-7	
23. Programming error (flaws or bugs in custom code)	Threat is completely addressed.	CSC 6.1-9	*Note 2*
24. Misdelivery (direct or deliver to wrong recipient)	* Threat is partially addressed.	CSC 6.1, 15.5, 17.1-8	HR-6
25. Loss or misplacement	* Threat is partially addressed.	CSC 1.6, 3.13, 17.1, 17.5	HR-7

Top Seven Human Risks (HR)
1. Phishability
2. Not patching, or using outdated systems
3. Posting too much information about self or work
4. Reusing passwords across sites
5. Indiscriminate use of mobile media
6. Lack of situational awareness (believing they are not a target)
7. Accidental loss or disclosure of sensitive information

Note 1: None of the Top HR apply directly here, but additional training can mitigate this risk.
Note 2: Developer awareness training can help mitigate this risk