Recommendations for Minimizing the Risk of a Security Breach

1. Monitor and evaluate what is being posted online by the organization as well as the employees
2. Conduct initial background checks on employees during the onboarding process and then again when employees are promoted into positions of increased trust
3. Develop a classification system for information (i.e. confidential, sensitive, proprietary, restricted)
4. Establish clear policies and procedures regarding access and use of information
5. Destroy information/records which are no longer needed
6. Password hygiene
7. Dual factor authentication
8. Ongoing security awareness training for all employees/contractors
9. Employee testing – simulated social engineering attacks
10. Foreign travel pre-brief and post-debrief
11. Employee termination/exit briefs
12. Penetration testing
13. Red teaming

pgwarmka@counterintelligence-institute.com
703-819-0091
www.counterintelligence-institute.com

© 2022