SPECIAL REPORT

48 IDEAS FOR CREATING A SECURE WORKPLACE

INTRODUCTION

This Special Report is designed to provide you with a brief background about basic security issues, and then provide you with strategies for avoiding the most common problems that arise in the workplace.

There is extensive management literature related to **workplace security issues**, from *petty theft* to *security of computer information* and *trade secret protection*. Three areas are emphasized throughout the literature. Your company must: 1) maintain *internal security measures*; 2) *investigate* all allegations and rumors promptly; and 3) *discipline* any breach of company security. It is important that you let employees know, in no uncertain terms, that theft or security violations *will not be tolerated* and will result in immediate termination as well as possible criminal prosecution.

SOME FACTS AND FIGURES ABOUT SECURITY RISKS

- According to the Bureau of National Affairs, businesses losses from employee dishonesty run between **$15 billion** and **$25 billion** a year!

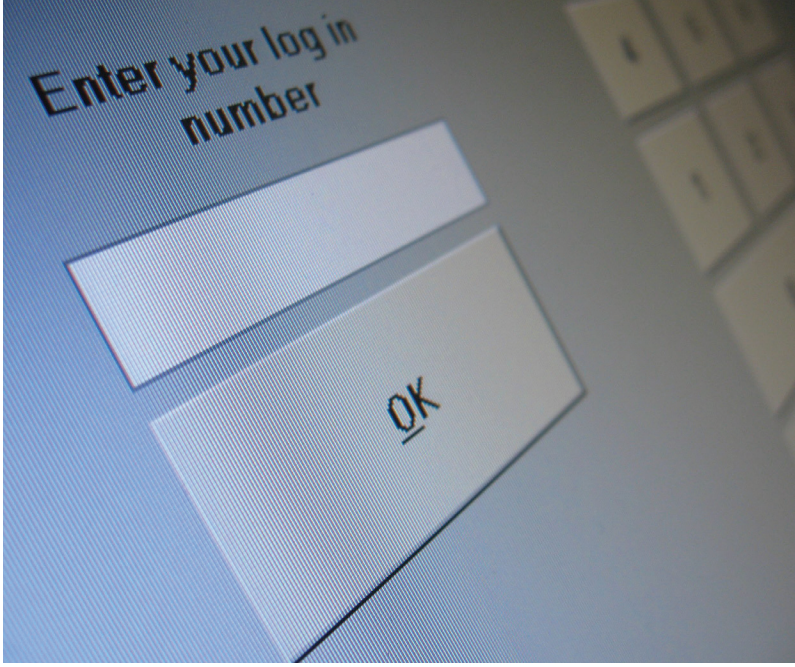
- The most frequently occurring business frauds are *credit card fraud*, *check fraud*, and *inventory theft*. Fraud such as *false financial statements, diversion of sales, kickbacks,* and *phantom vendors*, do not occur as often as other frauds, but when they do occur their economic impact is far more significant.

- A number of professional agencies in the security field estimate that between *10% to 30%* of all employees engage in what they broadly define as *employee theft*. Your company's exposure increases dramatically where there is no active preventative security measures employed.

donphin.com
619.852.4580 • don@donphin.com

© www.donphin.com

THINGS TO DO TO FOR A SECURE WORKPLACE:



Here are 48 ideas for you to consider:

1. Keep in mind that *anything* that can happen in the street can happen in the workplace!

2. *Put things away!* Use desk drawers, closets, and cabinets to reduce temptation and availability. Lock valuable items.

3. Make sure to maintain *control over access* to security passes, keys, security codes, etc.

4. Consider using security cameras, shopping services, computer scanning devices, etc. Provide *advance notice of any monitoring* and make sure it is directly related to a *legitimate business interest*.

5. Be very careful when using surveillance cameras in areas where employees or customers may have an expectation of *privacy*, such as changing rooms, restrooms, etc.

6. When using *written screening tests*, make sure they are job related, check the providers' credentials, make sure they can testify as to the validity of the test and make sure results are kept confidential.

7. Since *false imprisonment* claims can result whenever persons are wrongfully held against their will, be very careful when using a "shopkeeper's privilege" or when detaining an employee. An employee who wants to leave a meeting should be told that they may do so but that it will be considered an act of insubordination and will result in discipline.

8. *Do not* offer or give a *polygraph* examination under any circumstances without speaking with your lawyer first!

9. When *investigating* fraud or theft claims, be careful about using names and hearsay accusations.

10. *Be careful about threatening criminal prosecution*. This may be considered *extortion* or *blackmail* and get you into hot water.

11. It is appropriate to demand the *return* of any stolen property, as well as *restitution* for the items stolen.

12. Be aware of a high number of *refunds to customers* and safeguard against phantom refunds by using checks or merchandise credit for those refunds.

13. Statistics show a much lower rate of dishonesty when employees are paid a fair salary.

14. Use *inventory check out sheets* where possible.

15. Be aware of the potential for *collusion* between employees and management or employees and third parties related to fraud and security issues.

16. In all cases where there is sufficient evidence, have a security violations and fraud prosecuted.

17. Remember that very often an employee will admit to a smaller theft before they will admit to a larger one.

18. *Audit and monitor* long distance telephone bill records, computer use, and mail use on a random basis. Don't dig into private, non-work related communications.

19. Carefully *monitor expense accounts*, especially for car rentals, airline fares, transportation between the airports and meetings, and meal charges.

20. Put *supply cabinets* in easy *view* of supervision. Offer the supplies at your cost. Give them away as a value-added bonus at the beginning of the school year.

21. Have the company's *logo* or *name etched* into as many items as possible.

22. An employee who never seems to take a leave and puts in more time than a job requires, is a classic theft suspect. They will usually strongly object to procedural changes without apparent reason.

23. Consider *bonding employees*. 3-D Bonding covers dishonesty, disappearance, and destruction.

24. Do not use pre-printed signatures on checks.

25. Be aware of exorbitant postage use during the holiday season. Consider locking postage meters at night to prevent unauthorized use.

26. Have your *shipping records checked* on a regular basis to guard against *duplicate invoice numbers, un-invoiced shipments, inflated shipments*, etc.

27. *Investigate customer complaints* about non-receipt of goods promptly and thoroughly, as it may be an indication of fraud.

28. Inform employees and customers that you may sometimes tap into their telephone conversations to assure the quality of customer service. This *eavesdropping* is legal only when the participants are informed of it in advance. See the sample Voicemail/e-mail/ Internet policy.

29. Inform employees that all company property, including lockers, is subject to *random inspections.*

30. Set a firm policy against cashing checks or making small loans to employees out of petty cash.

31. Be aware of employees who appear to be living well beyond their means. If an employee's lifestyle cannot be supported by their salary then they are the most obvious and easiest risk to identify.

32. Be aware of the *financially irresponsible employee* who is unable to handle his or her own financial affairs properly. Do pre-hire investigations through Global HR Research and other agencies for those who handle accounts.

33. *Back up computer data* on a regular basis.

34. Provide a *fireproof safe* for backed up computer data and other valuable documents and items.

35. Participate in a *neighborhood watch* program.

36. Be aware of fraud or theft issues when dealing with employees *terminated* on an individual basis or during downsizing and lay off operations.

37. Be aware of the employee who engages in *compulsive gambling*, persistent *borrowing*, and the constant requesting of *advances*.

38. Conduct *immediate investigations* into safety and security claims and engage in appropriate discipline when necessary. Most fraud and safety violations are allowed to take place because of either *poor internal controls* or the *management override of internal controls*.

39. Remember that if you are a *unionized* company or utilize union workers, company policies may be subject to a bargaining agreement. When a unionized employee reasonably believes an investigation related to theft, security, safety, or other concern by the company may lead to discipline and they ask for union representation during the interview, it is an unfair labor practice for management to continue the interview without such representation.

40. Consider taking *two company representatives* into any security investigation so that one representative can take notes and act as a witness while the other asks the questions necessary.

41. Before disciplining an employee for security, fraud, theft, or other issues, find out if there are *extenuating circumstances* that might call for compassion and forgiveness.

42. Be aware of employees who have *alcohol* or *drug abuse problems*. They are one of the primary causes of security issues in the workplace.

43. Maintain *written company policies* related to security issues and communicate these policies to the employees. See the personnel forms in HR That Works.

44. Display *posters*, *slogans*, and other written materials to remind employees of security issues.

45. Make an effort to have *adequate lighting* both inside and outside your company facilities, especially in the parking lot area, entrances and exits.

46. See the Special Report: *19 Powerful Strategies for Investigating* and Managing Wrongful Employee Conduct.

47. See the Violence in the Workplace Training Module on HR That Works.

48. Check out The National Security Institute [www.nsi.org]. Aimed at the security professional; this site has a wealth of information.

CONCLUSION

The world is getting even more complex and your cyber liability and other security exposures are too. The above suggestions should be coupled with professional assistance and proper insurance coverage.

donphin.com
619.852.4580 • don@donphin.com